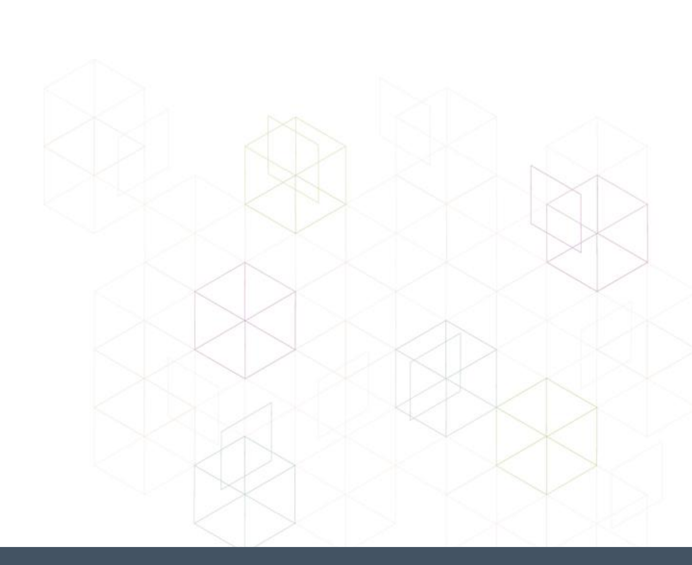


Nessus 5.2 HTML5-Benutzerhandbuch

16. Januar 2014

(Revision 20)



Inhaltsverzeichnis

Einleitung

Das vorliegende Dokument beschreibt die Verwendung der **Nessus-Benutzeroberfläche (UI)** von Tenable Network Security. Wir freuen uns über Ihre Anmerkungen und Vorschläge. Senden Sie diese an support@tenable.com.

Die Nessus-Benutzeroberfläche ist eine webbasierte Oberfläche für den Nessus-Sicherheitslückenscanner. Zur Verwendung der UI muss ein betriebsbereiter Nessus-Scanner in Ihrer Umgebung vorhanden sein, und Sie müssen mit der Bedienung des Scanners vertraut sein.

Regeln und Konventionen

In der gesamten Dokumentation werden Dateinamen, Daemons und ausführbare Dateien in einer Schriftart wie **`courier bold`** angezeigt (z. B.: **`gunzip`**, **`httpd`** oder **`/etc/passwd`**).

Befehlszeilenoptionen und Schlüsselwörter werden ebenfalls in der Schriftart **`courier bold`** angezeigt. Die Befehlszeilen sind teils mit, teils ohne Befehlszeilen-Prompt und den Ausgabetext des betreffenden Befehls aufgeführt. In den Befehlszeilen erscheint der ausgeführte Befehl in der Schriftart **`courier bold`**, um zu verdeutlichen, was der Benutzer eingegeben hat. Die vom System generierte Beispielausgabe ist hingegen in der Schriftart `courier` (ohne Fettdruck) aufgeführt. Es folgt ein Beispiel für die Ausführung des UNIX-Befehls **`pwd`**:

```
# pwd
/opt/nessus/
#
```



Wichtige Hinweise und Aspekte werden durch dieses Symbol und graue Textfelder hervorgehoben.



Tipps, Beispiele und Best Practices (Empfehlungen) werden durch dieses Symbol und weißen Text auf blauem Grund hervorgehoben.

Neues in Nessus 5.2

Seit dem 22. August 2013 haben die Nessus-Produkte folgende neue Namen:

Ehemaliger Produktname	Neuer Produktname
Nessus ProfessionalFeed	Nessus
Nessus HomeFeed	Nessus Home

Folgende Aufstellung zeigt die offiziellen Nessus-Produktnamen:

- Nessus®
- Nessus Perimeter Service
- Nessus Auditor Bundles
- Nessus Home

Die Nessus-Benutzeroberfläche im Überblick

Beschreibung

Die Nessus-Benutzeroberfläche (User Interface, UI) ist eine webbasierte Oberfläche für den Nessus-Scanner. Sie umfasst einen einfachen HTTP-Server und -Webclient und erfordert abgesehen vom Nessus-Server keine weitere Softwareinstallation. Seit Nessus 4 weisen alle Plattformen dieselbe Codebasis auf. Hierdurch werden nicht nur die meisten plattformspezifischen Bugs und Fehler beseitigt, sondern es wird auch eine schnellere Bereitstellung neuer Funktionen ermöglicht. Die wesentlichen Merkmale sind:

- Generierung von **`.nessus`**-Dateien, die von Tenable-Produkten standardmäßig als Grundlage für Informationen zu Sicherheitslücken und Scanrichtlinien verwendet werden
- In einer einzigen **`.nessus`**-Datei lassen sich eine Richtliniensitzung, eine Liste mit Zielen und die Ergebnisse mehrerer Scans speichern und problemlos exportieren. Weitere Informationen entnehmen Sie dem Leitfaden „Nessus v2 File Format“ („Nessus 2-Dateiformat“).
- Die Benutzeroberfläche zeigt Scanergebnisse in Echtzeit an. Sie müssen also nicht warten, bis ein Scan abgeschlossen ist, um die Resultate aufzurufen.
- Unabhängig von der Basisplattform wird eine einheitliche Oberfläche für den Nessus-Scanner bereitgestellt. Unter Mac OS X, Windows und Linux ist jeweils derselbe Leistungsumfang vorhanden.
- Die Ausführung von Scans auf dem Server wird nicht unterbrochen, wenn Ihre Verbindung aus irgendeinem Grund getrennt wird.
- Nessus-Scanberichte können über die Nessus-Benutzeroberfläche hochgeladen und mit anderen Berichten verglichen werden.
- Richtlinien-Assistent zur einfachen Erstellung von Scanrichtlinien für Audits in Ihrem Netzwerk

Unterstützte Plattformen

Da die Nessus-Benutzeroberfläche ein webbasierter Client ist, kann sie auf jeder Plattform ausgeführt werden, die einen Webbrowser bereitstellt.



> Die webbasierte Nessus-Benutzeroberfläche bietet maximale Leistung bei Verwendung von Microsoft Internet Explorer 10, Mozilla Firefox 24, Google Chrome 29, Opera 16 oder Apple Safari 6 auf dem Desktop. Zudem ist Nessus mit Chrome 29 für Android sowie mit Browsern unter iOS 7 kompatibel.



> Die webbasierte Nessus-Benutzeroberfläche erfordert zumindest Version 9 von Microsoft Internet Explorer.

Installation

Die Benutzerverwaltung des Nessus 5-Servers erfolgt nur noch über eine Weboberfläche oder SecurityCenter. Der vormalige NessusClient wird nicht mehr aktualisiert oder unterstützt.

Weitere Informationen zur Installation von Nessus finden Sie im Nessus 5.2-Installations- und Konfigurationshandbuch. Ab Nessus 5.0 ist Oracle Java (vormals Sun Microsystems Java) für die Generierung von PDF-Berichten erforderlich.

Bedienung

Übersicht

Nessus stellt eine einfache, aber leistungsfähige Oberfläche zur Verwaltung der Scanaktivitäten bereit.

Verbindung mit der Nessus-Benutzeroberfläche herstellen

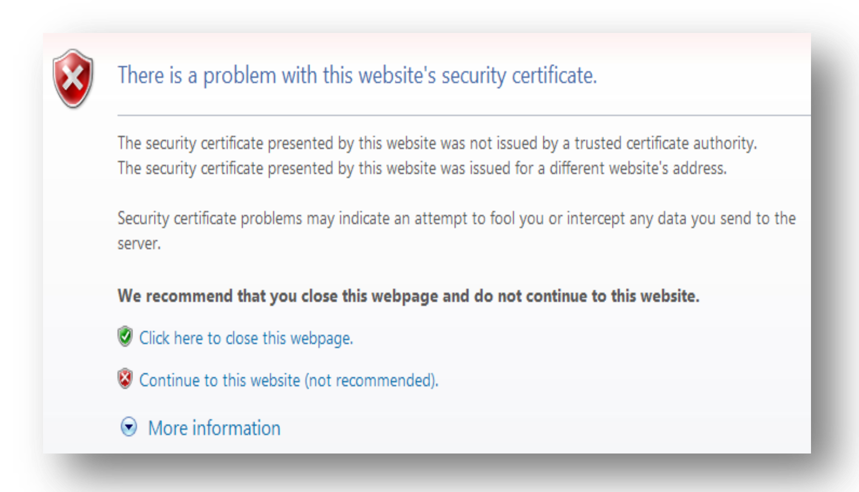
Führen Sie die folgenden Schritte aus, um die Nessus HTML5-Benutzeroberfläche zu starten:

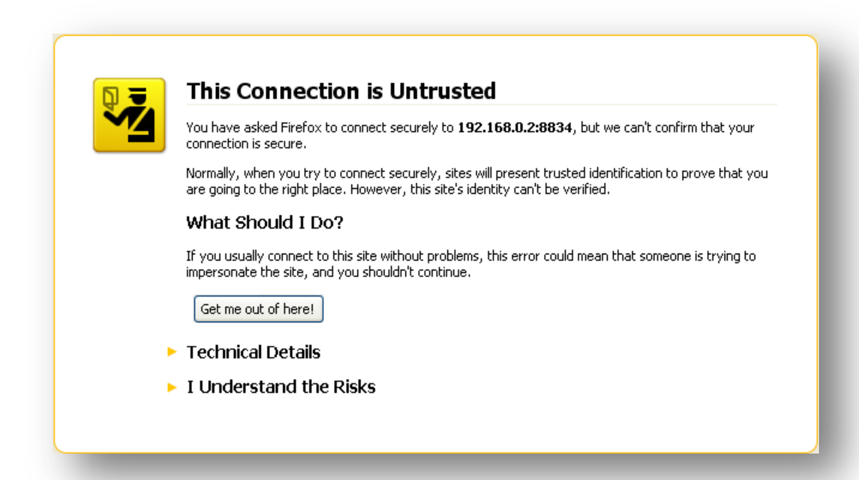
- Öffnen Sie einen beliebigen Webbrowser.
- Geben Sie `https://[Server-IP-Adresse]:8834/` in die Navigationsleiste ein.



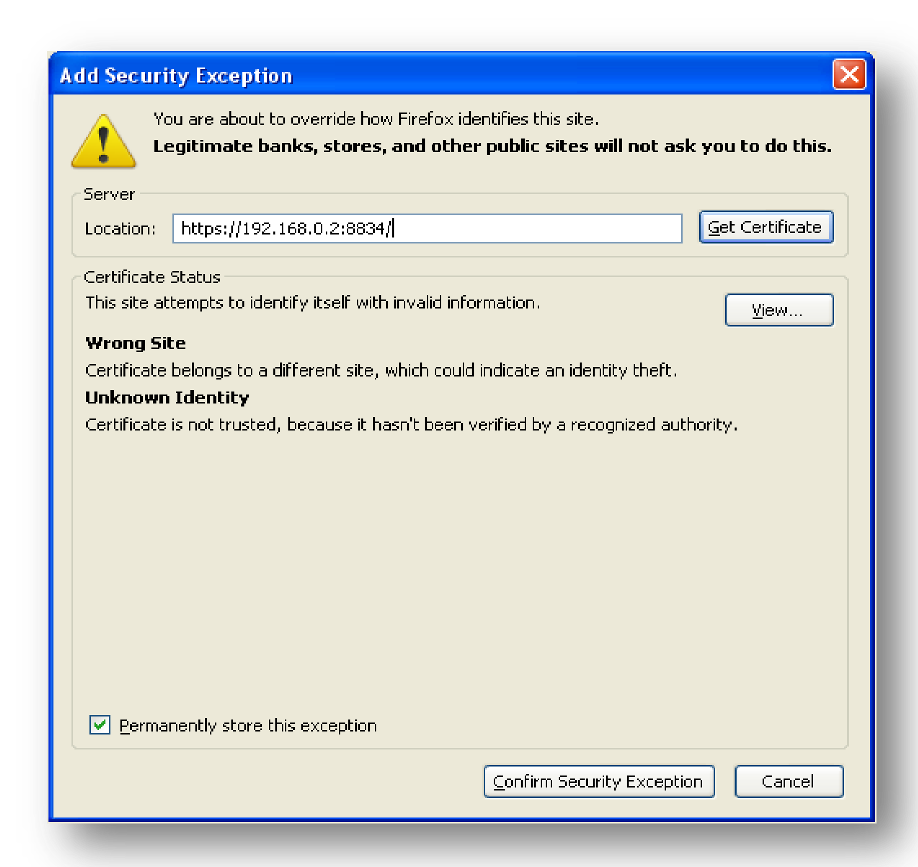
Achten Sie in jedem Fall darauf, die Verbindung mit der Benutzeroberfläche über HTTPS herzustellen, da nicht verschlüsselte HTTP-Verbindungen nicht unterstützt werden.

Wenn Sie zum ersten Mal eine Verbindung mit der Nessus-Benutzeroberfläche herstellen, zeigen die meisten Webbrowser eine Fehlermeldung an, laut der die Website nicht vertrauenswürdig ist, weil das SSL-Zertifikat selbstsigniert ist:



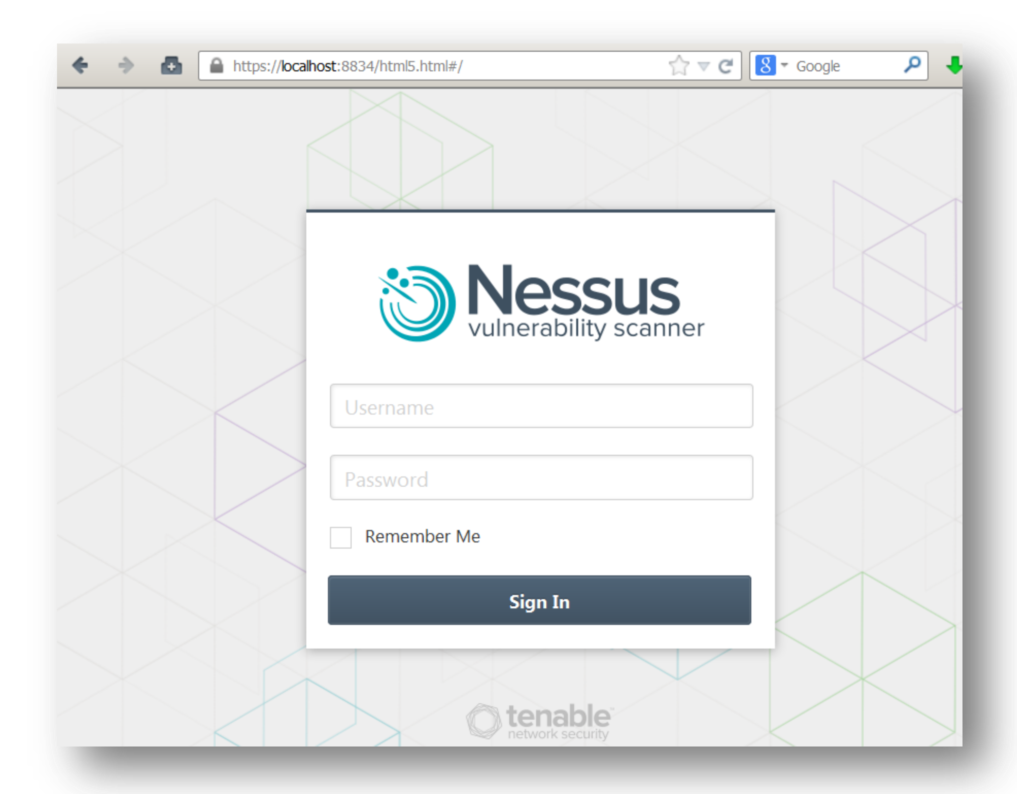


Benutzer von Microsoft Internet Explorer können auf „**Laden dieser Website fortsetzen (nicht empfohlen)**“ klicken, um die Nessus-Benutzeroberfläche zu laden. Benutzer von Firefox klicken auf „**Ich kenne das Risiko**“ und dann auf „**Ausnahme hinzufügen**…“, um das Dialogfeld „Sicherheits-Ausnahmeregel hinzufügen“ aufzurufen:

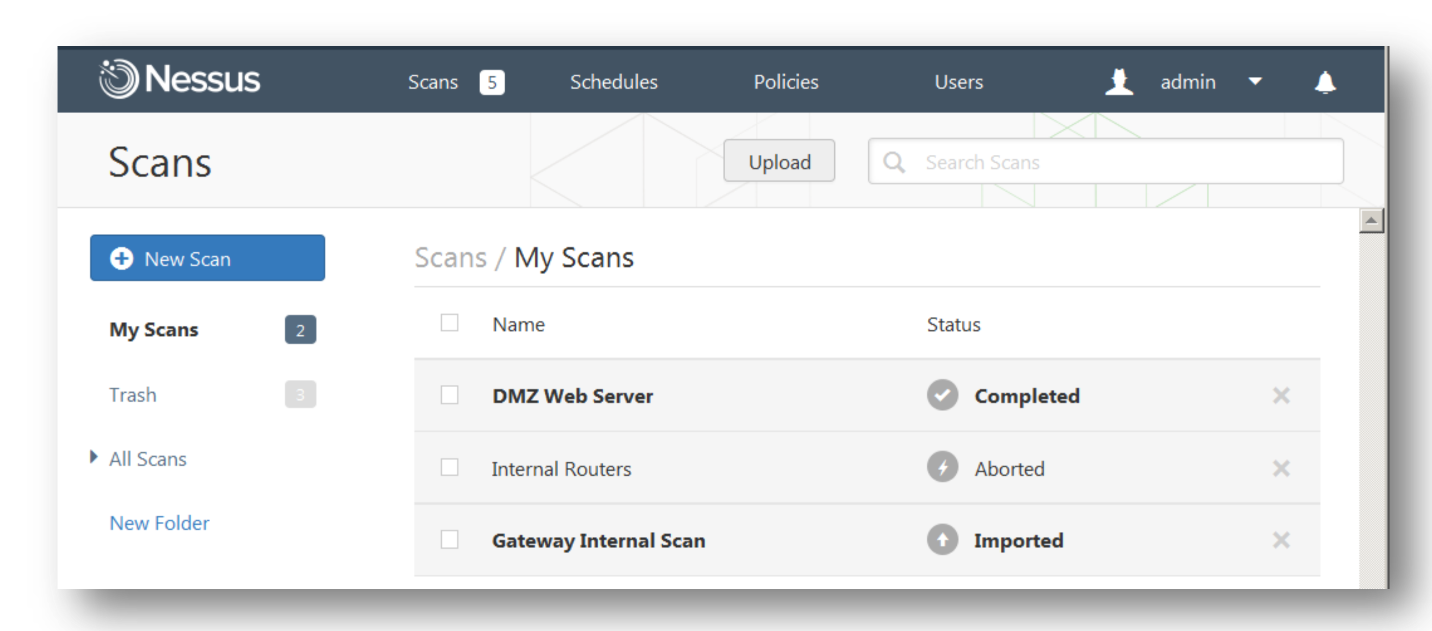


Vergewissern Sie sich, dass im Feld „Adresse“ die URL des Nessus-Servers steht, und klicken Sie auf „**Sicherheits-Ausnahmeregel bestätigen**“. Weitere Informationen zur Installation eines angepassten SSL-Zertifikats entnehmen Sie dem „Nessus-Installations- und Konfigurationshandbuch“.

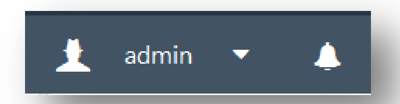
Nachdem die Ausnahme in Ihrem Browser bestätigt wurde, wird das folgende Startfenster angezeigt:



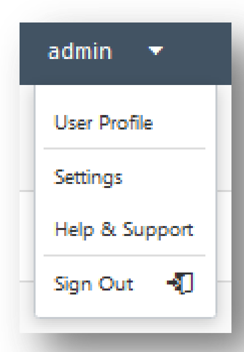
Authentifizieren Sie sich mithilfe des Benutzernamens und des Kennworts, das Sie zuvor mit dem Server Manager erstellt haben. Bei der Anmeldung können Sie den Browser auf Wunsch anweisen, den Benutzernamen auf dem Computer zu speichern. Verwenden Sie diese Option nur, wenn Ihr Computer sich stets in einer sicheren Umgebung befindet! Nach erfolgreicher Authentifizierung erscheinen auf der Benutzeroberfläche die Menüs zur Suche nach Berichten, zum Durchführen von Scans und zur Verwaltung der Richtlinien. Administratoren werden zudem Optionen der Benutzerverwaltung und Konfigurationsoptionen für den Nessus-Scanner angezeigt:



Die oben links gezeigten Menüoptionen sind zu jedem Zeitpunkt der Benutzung von Nessus verfügbar. Die Bezeichnung „admin“ im Dropdownmenü oben rechts in der oben gezeigten Bildschirmabbildung weist auf das aktuell angemeldete Konto hin. Ferner ist ein Glockensymbol für den Schnellzugriff auf wichtige Mitteilungen zum Nessus-Betrieb vorhanden:

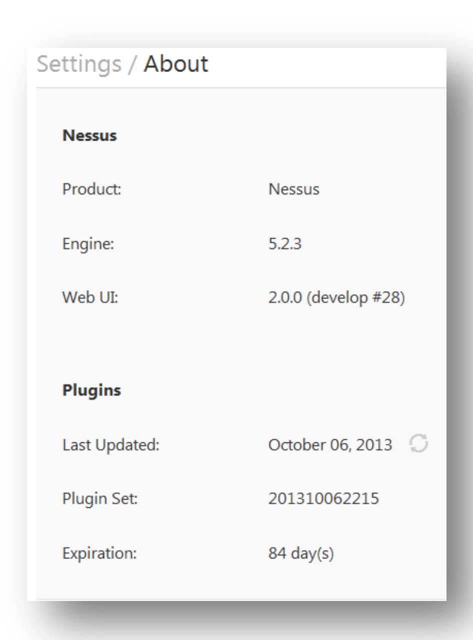


Durch Anklicken des Abwärtspfeils werden ein Menü für den Zugriff auf das Benutzerprofil, allgemeine Nessus-Einstellungen, Informationen zur Installation, Hilfe- und Supportoptionen sowie der Möglichkeit zum Abmelden angezeigt.



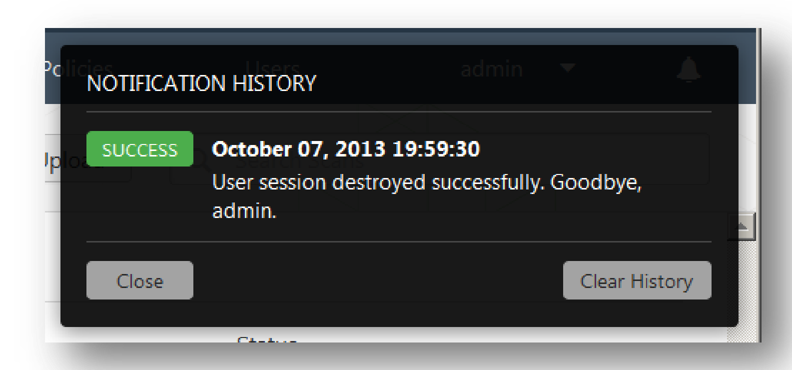
Die Option „**User Profile**“ („Benutzerprofil“) zeigt ein Menü mit mehreren Seiten zum Benutzerkonto an. Hierzu gehören Seiten zur Kennwortrücksetzung, zur Ordnerverwaltung und zur Konfiguration der Plugin-Richtlinien. Weitere Informationen zu diesen Optionen finden Sie weiter unten.

Die Option „**Settings**“ („Einstellungen“) gibt Ihnen Zugriff auf die Seite „**About**“ („Info“), die Konfigurationsoptionen des Mailservers (nur Administratoren), das Plugin-Feed (nur Administratoren) und erweiterte Scanneroptionen (nur Administratoren). Weitere Informationen zu diesen Optionen finden Sie weiter unten.

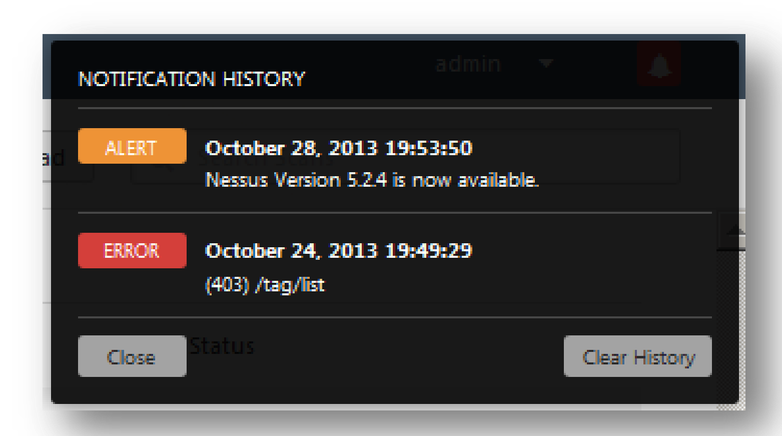


Über den Link „**Help & Support**“ („Hilfe und Support“) wird die Tenable-Supportseite in einer neuen Registerkarte oder einem neuen Fenster geladen. „**Sign Out**“ („Abmelden“) beendet die aktuelle Nessus-Sitzung.

Das Glockensymbol oben rechts kann angeklickt werden, um Mitteilungen zum Nessus-Betrieb (Fehler, Hinweise auf neue Nessus-Versionen, Sitzungsereignisse usw.) anzuzeigen:

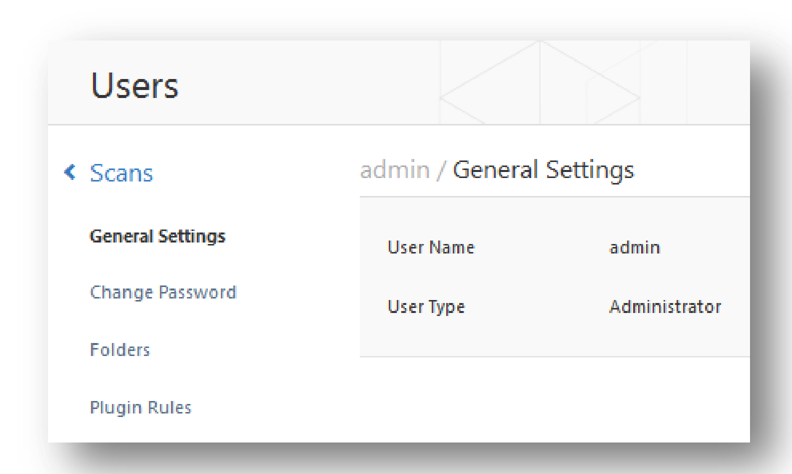


Hier werden Ihnen auch weitere Warnhinweise oder Fehler als Popupmeldungen angezeigt, die kurz nach Erscheinen wieder ausgeblendet werden. Sie verbleiben im Benachrichtigungsverlauf, bis sie gelöscht werden:



Benutzerprofil

In den Benutzerprofiloptionen können Sie Optionen zu Ihrem Konto bearbeiten.



Das Feld „**General Settings**" („Allgemeine Einstellungen") zeigt den gegenwärtig authentifizierten Benutzer sowie den Benutzertyp, also Administrator oder Benutzer.

Mit der Option „**Change Password**" („Kennwort ändern") können Sie Ihr Kennwort ändern. Dies wird generell alle drei Monate empfohlen.

Die Option „**Folders**" („Ordner") gibt Ihnen die Möglichkeit, die zur Speicherung der Scanergebnisse verwendeten Ordner zu verwalten. Auf diese Weise lässt sich die Speicherung der Scanergebnisse übersichtlich gestalten.

Mit der Option „**Plugin Rules**" („Plugin-Regeln") können Sie eine Sammlung von Richtlinien erstellen, die das Verhalten bestimmter Plugins zum jeweils ausgeführten Scan bestimmen. Richtlinien können auf dem Host (oder allen Hosts), der Plugin-ID, einem optionalen Ablaufdatum oder einer Änderung des Schweregrads beruhen. Dieselben Richtlinien können auch auf der Scanergebnisseite festgelegt werden.

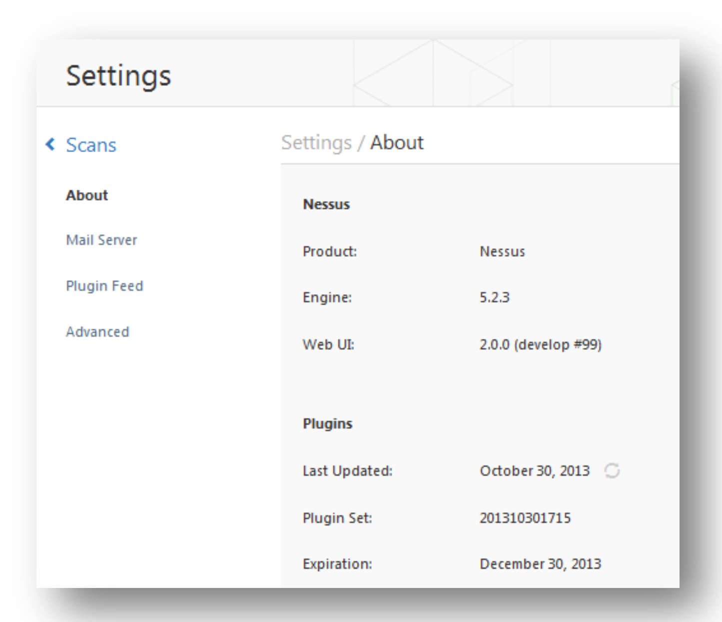
Einstellungen

Der Abschnitt „About" („Info") enthält Angaben über die Nessus-Installation. Hierzu gehören die Engine-Version, die Web-UI-Version, das Plugin-Aktualisierungsdatum, die Version der Plugin-Sammlung und das Ablaufdatum des Feeds.

Mit der Einstellung „Mail Server" („Mailserver") werden die SMTP-Servereinstellungen gesteuert. Weitere Informationen finden Sie im „Nessus 5.2-Installations- und Konfigurationshandbuch".

Mit der Einstellung „Plugin Feed" („Plugin-Feed") können Sie einen angepassten Plugin-Aktualisierungshost (z. B. für Offlineaktualisierungen über einen zentralen internen Server) und einen Proxy für Pluginaktualisierungen angeben. Weitere Informationen finden Sie im „Nessus 5.2-Installations- und Konfigurationshandbuch".

Der Abschnitt „Advanced" („Erweitert") enthält eine Vielzahl von Konfigurationsoptionen, die eine sehr fein abgestufte Steuerung des Scannerbetriebs ermöglichen. Weitere Informationen finden Sie im „Nessus 5.2-Installations- und Konfigurationshandbuch".



Tastenkombinationen für die Benutzeroberfläche

Die HTML5-Oberfläche verwendet eine Reihe von Tastenkombinationen, mit denen Sie schnell zu den Hauptbereichen der Benutzeroberfläche navigieren und häufig verwendete Aktionen ausführen können. Diese Tastenkombinationen stehen Ihnen jederzeit überall auf der Benutzeroberfläche zur Verfügung:

UI-Hauptfenster	
R	Results (Ergebnisse)
S	Scans
T	Templates (Vorlagen)
P	Policies (Richtlinien)
U	Users (Benutzer)
C	Configuration (Konfiguration)
Umschalttaste + Links-/Rechtspfeiltaste	Zwischen Registerkarten wechseln
Umschalttaste + S	Neuer Scan
Listenansichten	
Umschalttaste + Aufwärts-/Abwärtspfeiltaste	Auswahl nach oben oder unten verschieben
Umschalttaste + Eingabetaste	Gewählten Eintrag öffnen

Ergebnisansicht	
Umschalttaste + U	Bericht hochladen
Esc	Zurück zur Ergebnisliste
Links-/Rechtspfeiltaste	Vorherige bzw. nächste Sicherheitslücke im Detailmodus
D	Gewähltes Ergebnis löschen
Scanansicht	
N	Neuer Scan
Richtlinienansicht	
Umschalttaste + U	Neue Richtlinie hochladen
Benutzeransicht	
N	Neuer Benutzer

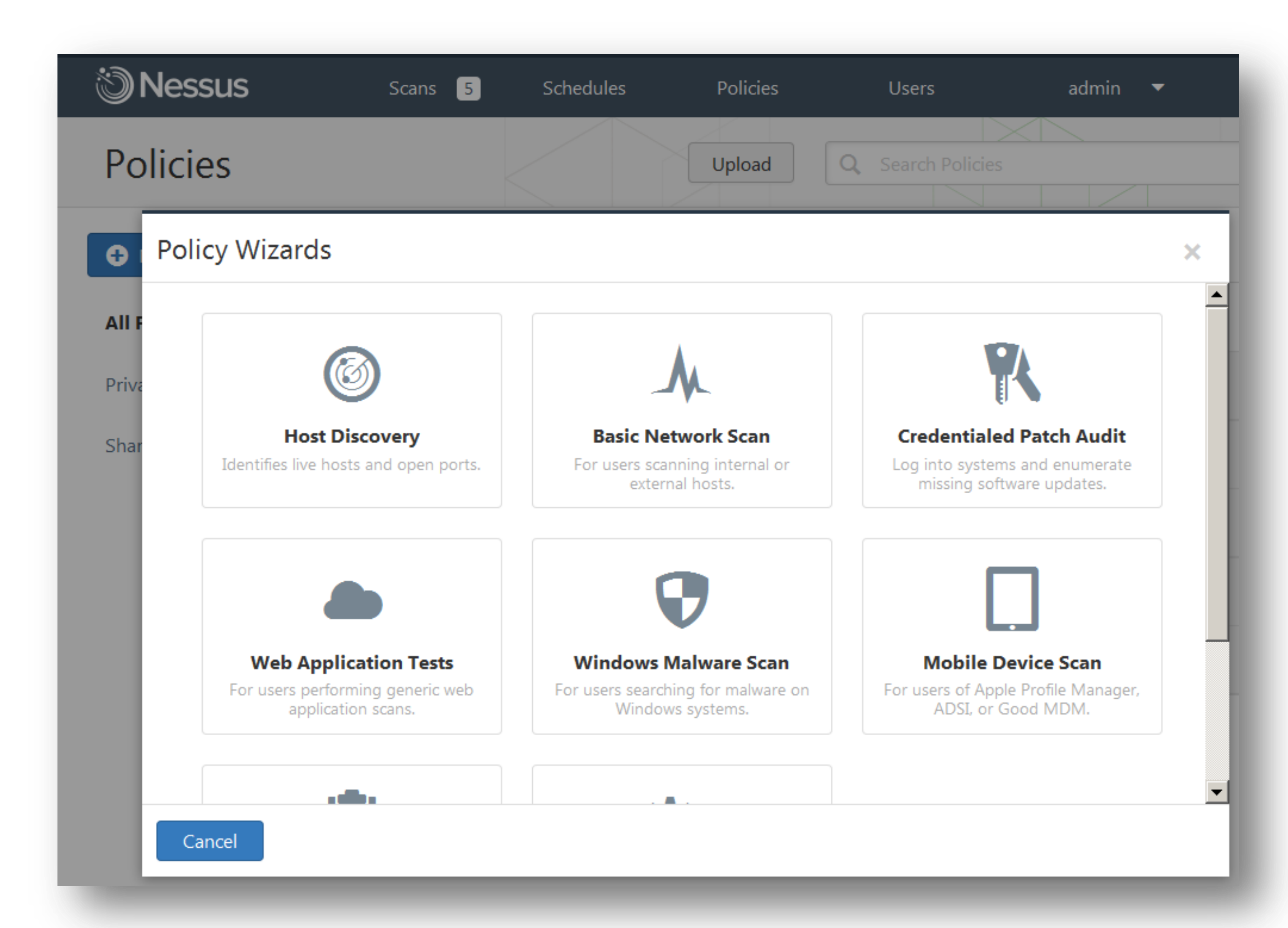
Überblick zu den Richtlinien

Eine Nessus-Richtlinie umfasst Konfigurationsoptionen für die Durchführung von Sicherheitslückenscans. Hierzu zählen unter anderem:

- Parameter zur Steuerung technischer Aspekte des Scans (z. B. Timeouts, Anzahl der Hosts, Art des Portscanners usw.)
- Anmeldedaten für lokale Scans (z. B. Windows, SSH), authentifizierte Oracle-Datenbankscans, HTTP, FTP, POP, IMAP oder eine Kerberos-basierte Authentifizierung
- Spezifikationen für abgestufte Scans auf Basis von Plugins oder Plugin-Familien
- Tests der Compliancerichtlinien für Datenbanken, Ausführlichkeit von Berichten, Scaneinstellungen für die Diensterkennung, UNIX-Compliancetests usw.

Neue Richtlinie erstellen

Wenn Sie eine Verbindung mit einer Nessus-Serverbenutzeroberfläche hergestellt haben, können Sie eine angepasste Richtlinie erstellen. Hierzu klicken Sie auf die Option „**Policies**“ („Richtlinien“) oben in der Menüleiste und dann rechts auf die Schaltfläche „**+ New Policy**“ („+ Neue Richtlinie“). Das Fenster zum Hinzufügen der Richtlinie erscheint:



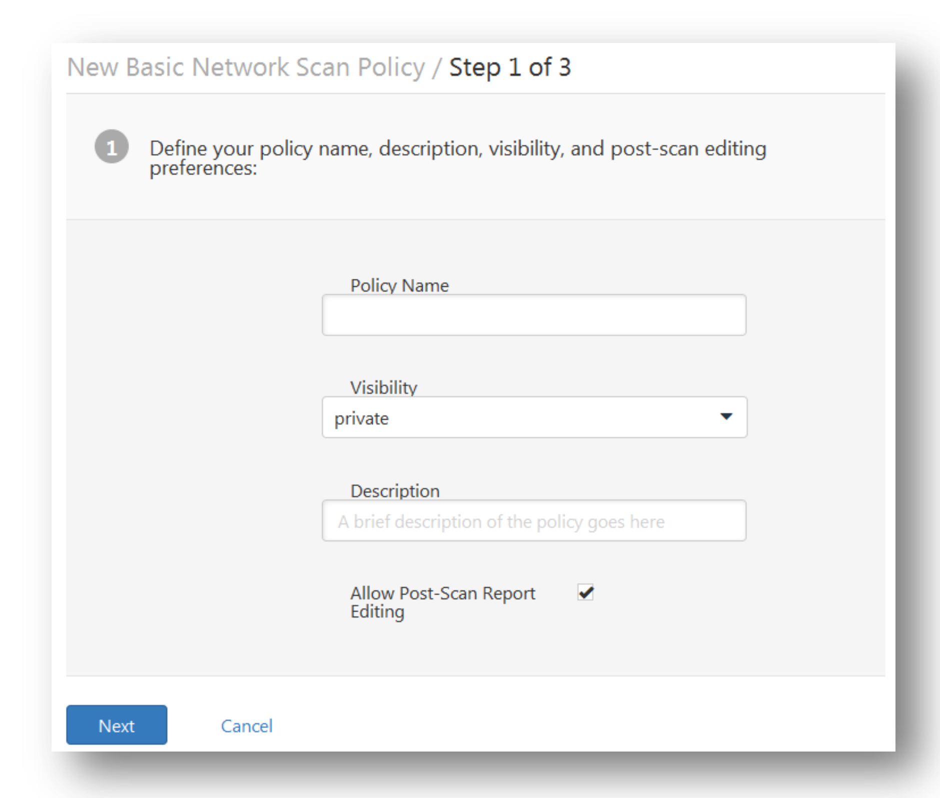
Mit dem Richtlinien-Assistenten arbeiten

Die erste Option ist der optionale Einsatz des Richtlinien-Assistenten zur Erstellung einer Richtlinie mit bestimmtem Zweck. Der Assistent bietet folgende Standardvorlagen:

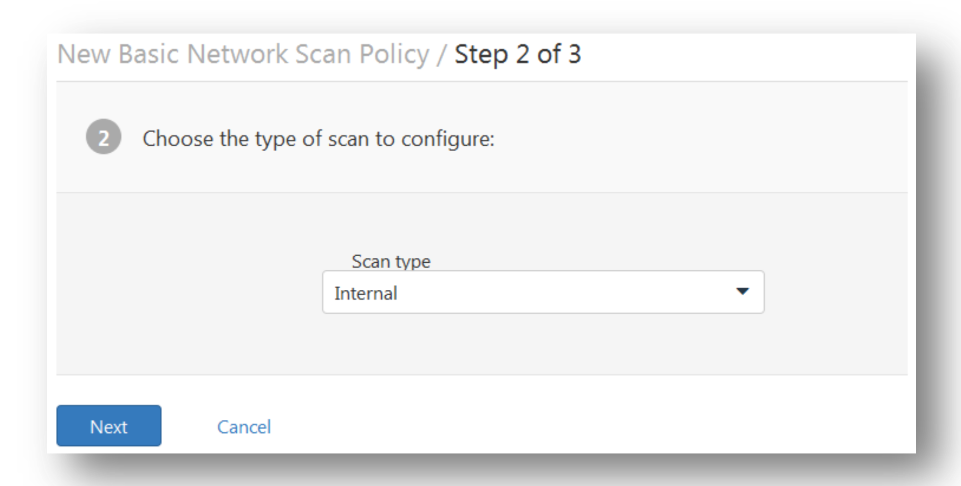
Name des Richtlinien-Assistenten	Beschreibung
Host Discovery (Hosterkennung)	Identifiziert Hosts, die online sind, und offene Ports.
Basic Network Scan (Einfacher Netzwerkscan)	Zum Scannen interner oder externer Hosts
Credentialed Patch Audit (Patch-Audit mit Authentifizierung)	Anmeldung auf Systemen und Auflistung fehlender Softwareaktualisierungen
Web Application Tests (Webanwendungstests)	Für Benutzer, die generische Webanwendungsscans durchführen

Windows Malware Scan (Windows-Malwarescan)	Für Benutzer, die nach Malware auf Windows-Systemen suchen
Mobile Device Scan (Scan von Mobilgeräten)	Für Benutzer von Apple Profil-Manager, ADSI oder Good MDM
Prepare for PCI DSS Audits (Vorbereitung auf PCI-DSS-Audits)	Für Benutzer, die ein PCI-DSS-Compliance-Audit vorbereiten
Advanced Policy (Erweiterte Richtlinien)	Für Benutzer, die vollständige Kontrolle über ihre Richtlinienkonfiguration benötigen

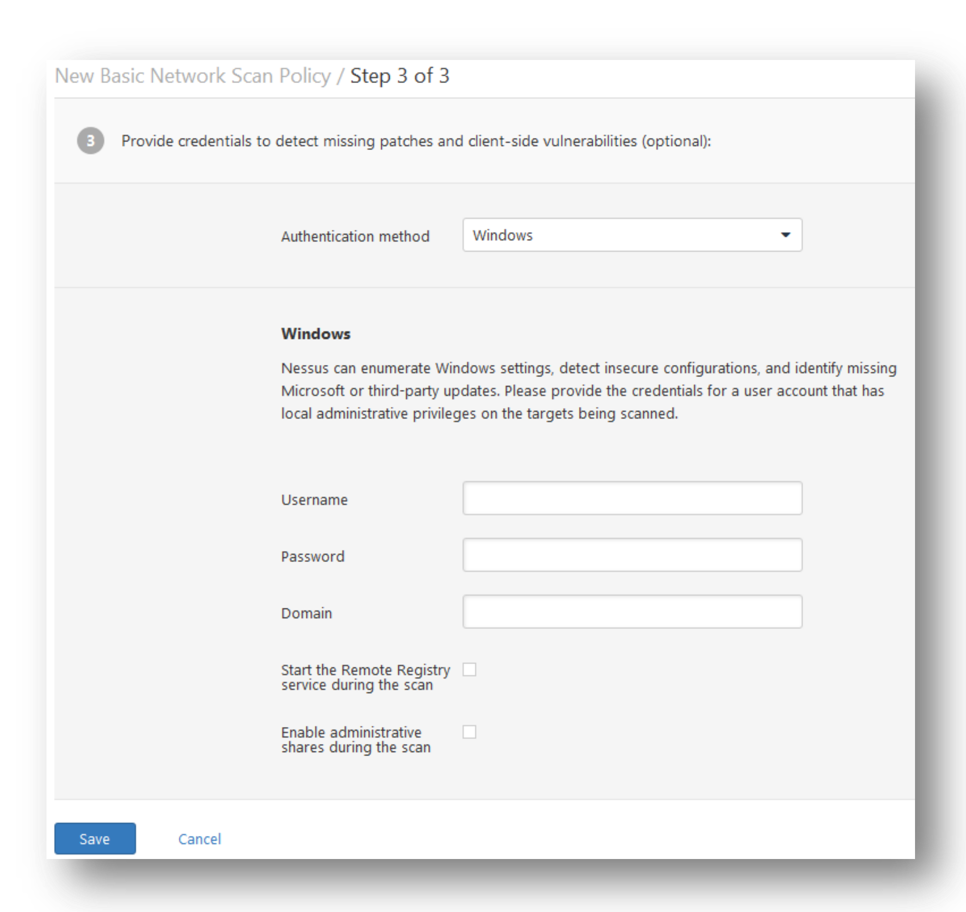
Zukünftig werden zur Verbesserung der Kundenfreundlichkeit im Richtlinien-Assistenten vorhandene Assistenten erweitert und neue Assistenten hinzugefügt werden. Nachfolgend wird die Verwendung eines Assistenten im Überblick beschrieben. Beachten Sie, dass jeder Assistent anders funktioniert – die beschriebene Vorgehensweise ist lediglich exemplarisch gedacht.



Im ersten Schritt des Assistenten werden Sie aufgefordert, der Richtlinie einen Namen zu geben, Angaben zur Sichtbarkeit (privat oder freigegeben) zu machen und eine Beschreibung einzugeben. Mit dem Assistenten erstellte Richtlinien ermöglichen grundsätzlich eine Bearbeitung des Berichts nach dem Scan. Klicken Sie auf „**Next**“ („Weiter“), um zum nächsten Schritt zu gelangen:



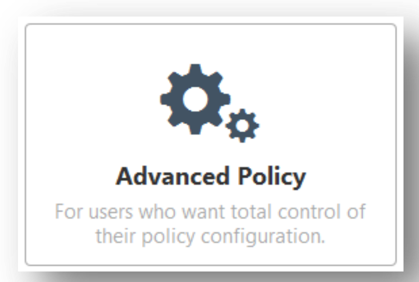
Hier müssen Sie festlegen, ob die Richtlinie für interne oder externe Hosts verwendet wird, da jeweils unterschiedliche Optionen zur Verfügung stehen. Klicken Sie auf „**Next**“, um zum abschließenden Schritt zu gelangen:



Im letzten Schritt haben Sie die Wahl, zum optimierten Scannen Anmeldedaten hinzuzufügen. Wie bereits erwähnt, sind einige Schritte im Assistenten optional. Nach der Erstellung wird die Richtlinie mit den empfohlenen Einstellungen gespeichert. Sie können die Optionen des Assistenten wie auch jeden anderen Aspekt der Richtlinie jederzeit bearbeiten.

Erweiterte Richtlinienerstellung

Wenn Sie den Richtlinien-Assistenten nicht verwenden möchten, können Sie mit der Option „Advanced“ („Erweitert“) eine Richtlinie auf herkömmliche Weise einrichten und haben von Anfang an vollständige Kontrolle über alle Einstellungen.



Hier finden Sie vier Registerkarten für die Konfiguration: „**General Settings**“ („Allgemeine Einstellungen“), „**Credentials**“ („Anmeldedaten“), „**Plugins**“ und „**Preferences**“ („Voreinstellungen“). Die Standardeinstellungen ermöglichen eine maximal abgestufte Kontrolle des Nessus-Scannerbetriebs und müssen für die meisten Umgebungen nicht geändert werden. Die Registerkarten sind nachfolgend beschrieben.

General Settings

Die Registerkarte „**General Settings**“ („Allgemeine Einstellungen“) erlaubt das Benennen der Richtlinie und die Konfiguration scanspezifischer Vorgänge. Das Scannerverhalten lässt sich über vier Dropdownmenüs steuern:

Im Bereich „**Basic**“ („Grundlagen“) definieren Sie Aspekte zur Richtlinie selbst:

Option	Beschreibung
Name	Hier wird der Name festgelegt, der zur Bezeichnung der Richtlinie auf der Nessus-Benutzeroberfläche verwendet wird.
Visibility (Sichtbarkeit)	Hierdurch wird bestimmt, ob die Richtlinie mit anderen Benutzern gemeinsam verwendet wird („*shared*“) oder Ihrem persönlichen Gebrauch vorbehalten bleibt („*private*“). Nur Administratoren können Richtlinien zur gemeinsamen Verwendung freigeben.
Description (Beschreibung)	Hier kann eine kurze Beschreibung der Scanrichtlinie eingegeben werden. Das Feld eignet sich normalerweise zur Zusammenfassung des allgemeinen Zwecks der Richtlinie (z. B. „Webserverscans ohne lokale Tests und Nicht-HTTP-Dienste“).
Allow Post-Scan Report Editing (Nachträgliche Bearbeitung von Berichten zulassen)	Mithilfe dieser Funktion kann der Benutzer Elemente aus dem Bericht löschen. Bei einem Compliance-Scan oder anderen Audits sollte die Option nicht markiert sein, um den Beweis einer manipulationsfreien Berichterstellung zu gewährleisten.

Über das Menü „**Port Scanning**“ („**Portscans**“) werden Portscanoptionen einschließlich Scans des Portbereichs und der Methoden gesteuert:

Option	Beschreibung
Port Scan Range (Bereich für Portscan)	Legt einen bestimmten Portbereich für den Scanner fest. Als Eingaben akzeptiert werden „default“ („Vorgabe“, umfasst die ca. 4.790 in der Datei `nessus-services` aufgeführten, häufig verwendeten Ports), „all“ („Alle“) zum Scannen aller 65.535 Ports

	oder aber eine benutzerspezifische Liste von Ports. Beispielsweise sind Angaben wie „21,23,25,80,110“ oder „1-1024,8080,9000-9200“ zulässig. Wenn Sie „1-65535“ festlegen, werden alle Ports gescannt. Sie können auch einen Teilbereich angeben, der für das jeweilige Protokoll spezifisch ist. Wenn Sie beispielsweise mit einer Richtlinie unterschiedliche Portbereiche für TCP und UDP scannen möchten, könnten Sie Folgendes angeben: „T:1-1024,U:300-500“. Des Weiteren können Sie eine Gruppe von Ports, die für beide Protokolle gescannt werden sollen, und zusätzlich Einzelbereiche für das jeweilige Protokoll angeben (z. B. „1-1024,T:1024-65535,U:1025“). Wenn Sie nur ein einziges Protokoll scannen möchten, wählen Sie lediglich den betreffenden Portscanner aus und geben die Ports wie üblich an.
Consider Unscanned Ports as Closed (Nicht gescannte Ports als geschlossen betrachten)	Wenn ein Port mit einem ausgewählten Portscanner nicht gescannt wird (weil er beispielsweise außerhalb des angegebenen Bereichs liegt), wird er von Nessus als geschlossen betrachtet.
Nessus SNMP Scanner	Hiermit wird Nessus angewiesen, Ziele auf das Vorhandensein eines SNMP-Diensts zu prüfen. Nessus versucht während eines SNMP-Scans, relevante Einstellungen zu erschließen. Wenn die Einstellungen durch den Benutzer unter „Preferences“ („Voreinstellungen“) angegeben wurden, kann Nessus den Remotehost besser testen und ausführlichere Auditresultate generieren. Es gibt beispielsweise eine ganze Reihe von Tests für Cisco-Router, mit denen durch Verarbeitung des zurückerhaltenen SNMP-Strings die vorhandenen Sicherheitslücken ermittelt werden. Diese Angaben sind für solche Audits erforderlich.
Nessus UDP Scanner	Verwendet den integrierten UDP-Scanner von Nessus zur Ermittlung offener UDP-Ports auf den Zielsystemen. UDP ist ein „zustandsloses“ Protokoll, d. h., die Kommunikation erfolgt nicht über Handshake-Dialoge. Die UDP-basierte Kommunikation ist nicht immer zuverlässig und aufgrund der Eigenschaften von UDP-Diensten und -Auslesegeräten auch nicht immer remote erkennbar.
Netstat Portscanner (SSH)	Diese Option nutzt `netstat` zur Prüfung auf offene Ports auf dem lokalen Computer. Hierzu wird auf den Befehl `netstat` zurückgegriffen, der über eine SSH-Verbindung zum Ziel verfügbar ist. Der Scan ist in erster Linie für Systeme auf UNIX-Basis gedacht und erfordert Anmeldedaten zur Authentifizierung.
Ping the remote host (Pingbefehl an Remotehost senden)	Diese Option ermöglicht das Senden von Pingbefehlen an Remotehosts über mehrere Ports, um festzustellen, ob sie online sind.
Netstat Portscanner (WMI)	Diese Option nutzt `netstat` zur Prüfung auf offene Ports auf dem lokalen Computer. Hierzu wird auf den Befehl `netstat` zurückgegriffen, der über eine WMI-Verbindung zum Ziel verfügbar ist. Der Scan ist in erster Linie für Windows-Systeme gedacht und erfordert Anmeldedaten zur Authentifizierung. Ein Scan auf WMI-Basis ermittelt mithilfe von `netstat` offene Ports, d. h., angegebene Portbereiche werden ignoriert. Wenn ein Port-Enumerator (`netstat` oder SNMP) erfolgreich ist, umfasst der Portbereich nachfolgend alle Ports (Einstellung „all“). Allerdings wird Nessus die Option „Consider Unscanned Ports As Closed“ („Nicht gescannte Ports als geschlossen betrachten“) berücksichtigen, sofern

	diese aktiviert ist.
Nessus TCP Scanner	Verwendet den integrierten TCP-Scanner von Nessus zur Ermittlung offener TCP-Ports auf den Zielsystemen. Dieser Scanner ist optimiert und verfügt über Selbstoptimierungsfunktionen. Auf einigen Plattformen (z. B. Windows oder Mac OS X) wird bei Auswahl dieses Scanners der SYN-Scanner verwendet, um schwerwiegende Leistungsprobleme zu vermeiden, die für die betreffenden Betriebssysteme spezifisch sind.
Nessus SYN Scanner	Verwendet den integrierten SYN-Scanner von Nessus zur Ermittlung offener TCP-Ports auf den Zielsystemen. SYN-Scans sind ein beliebter Ansatz zur Durchführung von Portscans und gelten im Vergleich zu TCP-Scans allgemein als weniger aggressiv. Der Scanner sendet ein SYN-Paket an diesen Port, wartet auf die SYN-ACK-Antwort und bestimmt den Portstatus anhand der Antwort bzw. anhand des Ausbleibens der Antwort.

Über die Option „**Port Scan Range**" („Portscanbereich") wird ein bestimmter Portbereich als Zielbereich festgelegt. Folgende Werte sind möglich:

Wert	Beschreibung
„default" („Standard")	Wenn das Schlüsselwort „**default**" angegeben wird, scannt Nessus ca. 4.790 häufig verwendete Ports. Die Liste dieser Ports kann der Datei `nessus-services` entnommen werden.
„all" („Alle")	Wenn das Schlüsselwort „**all**" angegeben wird, scannt Nessus alle 65.535 Ports.
Custom List (Benutzerdefinierte Liste)	Ein benutzerdefinierter Portbereich kann mithilfe einer Liste kommagetrennter Ports oder Portbereiche festgelegt werden. Beispielsweise sind Angaben wie „21,23,25,80,110" oder „1-1024,8080,9000-9200" zulässig. Wenn Sie „1-65535" festlegen, werden alle Ports gescannt. Sie können auch einen Teilbereich angeben, der für das jeweilige Protokoll spezifisch ist. Wenn Sie beispielsweise mit einer Richtlinie unterschiedliche Portbereiche für TCP und UDP scannen möchten, könnten Sie Folgendes angeben: „T:1-1024,U:300-500". Des Weiteren können Sie eine Gruppe von Ports, die für beide Protokolle gescannt werden sollen, und zusätzlich Einzelbereiche für das jeweilige Protokoll angeben (z. B. „1-1024,T:1024-65535,U:1025"). Wenn Sie nur ein einziges Protokoll scannen möchten, wählen Sie lediglich den betreffenden Portscanner aus und geben die Ports wie üblich an.

Im Bereich „**Performance**" („Leistung") sind zwei Optionen vorhanden, mit denen die Anzahl der zu startenden Scans gesteuert wird. Diese Optionen sind bei der Konfiguration eines Scans die vielleicht wichtigsten, denn sie haben die größten Auswirkungen auf Scandauer und Netzwerkaktivitäten.

Option	Beschreibung
Max Checks Per Host (Tests je Host maximal)	Mit dieser Einstellung wird die Anzahl der Tests begrenzt, die ein Nessus-Scanner gleichzeitig für einen einzelnen Host ausführt.
Max Hosts Per Scan (Hosts je Scan maximal)	Mit dieser Einstellung wird die Anzahl der Hosts begrenzt, die von einem Nessus-Scanner gleichzeitig gescannt werden.
Network Receive Timeout (Timeout für Netzwerkdatenempfang, in Sekunden)	Der Standardwert liegt bei fünf Sekunden. Angegeben wird, wie lange Nessus auf Antwort von einem Host wartet (sofern durch ein Plugin nichts anderes festgelegt ist). Wenn Sie über eine langsame Verbindung scannen, sollten Sie hier einen höheren Wert eingeben.
Max Simultaneous TCP Sessions Per Host (Gleichzeitige Anzahl TCP-Sitzungen je Host maximal)	Durch diese Einstellung kann die Anzahl gleichzeitig laufender TCP-Sitzungen für einen einzelnen Host beschränkt werden. Mithilfe dieser TCP-Drosselung steuern Sie auch die Anzahl der Pakete, die der SYN-Scanner am Ende pro Sekunde sendet (ist diese Option beispielsweise auf 15 festgelegt, dann sendet der SYN-Scanner maximal 1500 Pakete pro Sekunde).
Max Simultaneous TCP Sessions Per Scan (Gleichzeitige Anzahl TCP-Sitzungen je Scan maximal)	Durch diese Einstellung kann die Anzahl gleichzeitig laufender TCP-Sitzungen für den gesamten Scan beschränkt werden (die Anzahl der gescannten Hosts spielt hierbei keine Rolle). Bei Nessus-Scannern, die unter Windows XP, Vista, 7 oder 8 installiert sind, darf dieser Wert höchstens 19 betragen, da andernfalls keine korrekten Resultate zu erzielen sind.
Reduce Parallel Connections on Congestion (Parallele Verbindungen bei Überlast verringern)	Bei Aktivierung dieser Option kann Nessus erkennen, dass zu viele Pakete versendet werden und die maximale Kapazität der Netzwerkverbindung in Kürze erreicht werden wird. In diesem Fall drosselt Nessus die Scanrate, um die Überlastung zu mindern. Nach dem Verstreichen der Überlastung versucht Nessus automatisch, die verfügbare Kapazität der Netzwerkverbindung wieder optimal zu nutzen.
Use Kernel Congestion Detection (Linux only) (Kernel-Überlastungserkennung verwenden, nur Linux)	Ermöglicht Nessus die Überwachung der CPU und anderer interner Vorgänge auf Überlastung und eine ggf. erforderliche Verringerung der Verarbeitungs-geschwindigkeit. Nessus wird immer versuchen, möglichst alle verfügbaren Ressourcen zu verwenden. Diese Funktionalität ist nur für Nessus-Scanner verfügbar, die auf einem Linux-System installiert sind.

Im Menü „**Advanced**“ („Erweitert“) sind die Optionen in Zusammenhang mit dem Verhalten eines Scans weiter definiert:

Option	Beschreibung
Safe Checks (Sichere Tests)	„Safe Checks“ deaktiviert alle Plugins, die sich unter Umständen negativ auf den Remotehost auswirken können.
Silent Dependencies (Abhängigkeiten nicht aufführen)	Wenn diese Option aktiviert ist, wird die Liste der Abhängigkeiten nicht im Bericht aufgeführt. Soll die Liste der Abhängigkeiten im Bericht enthalten sein, dann müssen Sie das Kontrollkästchen deaktivieren.
Log Scan Details to Server (Scandetails auf Server	Hiermit werden zusätzliche Details des Scans in der Nessus-Serverlogdatei (`nessusd.messages`) gespeichert, z. B. der Start, die Beendigung oder der

protokollieren)	erzwungene Abbruch von Plugins. Anhand der resultierenden Logdatei können Sie nachprüfen, ob bestimmte Plugins verwendet und Hosts gescannt wurden.
Stop Host Scan on Disconnect (Hostscan bei Trennung beenden)	Wenn diese Option aktiviert ist, beendet Nessus den Scan, sobald erkannt wurde, dass der Host nicht mehr reagiert. Dies kann beispielsweise geschehen, wenn Benutzer den PC während eines Scans abschalten, ein Host nach Verwendung eines Denial-of-Service-Plugins nicht mehr reagiert oder ein Sicherheitsmechanismus (z. B. ein IDS) die Datenübertragung an den Server gesperrt hat. Würde der Scan solcher Computer fortgesetzt, so würde unnötiger Datenverkehr im Netzwerk übertragen, und der Scan würde verzögert.
Avoid Sequential Scans (Fortlaufende Scans vermeiden)	Standardmäßig scannt Nessus eine Liste mit IP-Adressen in fortlaufender Reihenfolge. Wenn jedoch diese Option aktiviert ist, scannt Nessus die Liste in zufälliger Reihenfolge. Dies ist normalerweise nützlich, um den an ein bestimmtes Subnetz gerichteten Datenverkehr besser zu verteilen, wenn der Scan umfangreich ist. Bis Juli 2013 funktionierte diese Option auf der Subnetzebene. Danach wurde die Funktion auf randomisierte Erfassung des gesamten IP-Zielbereichs erweitert.
Designate Hosts by their DNS Name (DNS-Namen für Hosts)	Wenn Sie diese Option auswählen, wird statt der IP-Adresse der Hostname in der Berichtsausgabe verwendet.



Der für einen Portscan angegebene Bereich ist gleichermaßen für TCP- und UDP-Scans gültig.

Credentials

Auf der nachfolgend abgebildeten Registerkarte „**Credentials**" („Anmeldedaten") können Sie die Verwendung von Authentifizierungsdaten für Scanvorgänge durch den Nessus-Scanner konfigurieren. Nach der Konfiguration dieser Informationen kann Nessus eine größere Zahl von Tests ausführen und gelangt so zu genaueren Ergebnissen.

Im Dropdownmenü „**Windows credentials**" („Windows-Anmeldedaten") sind Einstellungen enthalten, um Nessus Informationen wie den Namen, das Kennwort und den Domänennamen für das SMB-Konto zu übermitteln. SMB (Server Message Block) ist ein Dateifreigabeprotokoll, mit dem Computer Daten im gesamten Netzwerk transparent verwenden können. Mithilfe dieser Angaben kann Nessus lokale Daten über einen Windows-Remotehost suchen. Beispielsweise kann Nessus unter Verwendung der Authentifizierungsdaten feststellen, ob wichtige Sicherheitspatches bereits aufgespielt wurden. Die Standardwerte der anderen SMB-Parameter müssen nicht geändert werden.



Sind mehrere SMB-Konten konfiguriert, probiert Nessus die angegebenen Anmeldedaten bis zur erfolgreichen Anmeldung nacheinander aus. Nach erfolgreicher Authentifizierung mit einem Anmeldedatensatz prüft Nessus auch die übrigen angegebenen Anmeldedaten, verwendet sie aber nur, wenn diese Administratorzugriff gewähren, während die vorherigen Konten lediglich einen Benutzerzugriff gestatten.

Einige Windows-Versionen lassen die Einrichtung neuer Administratorkonten zu. Für authentifizierte Scans sind solche Konten jedoch nicht unbedingt geeignet. Tenable empfiehlt für authentifizierte Scans die Verwendung des ursprünglichen Administratorkontos („Administrator"), um vollen Zugriff zu erhalten. Bei bestimmten Windows-Versionen ist dieses Konto möglicherweise ausgeblendet. Es lässt sich einblenden, indem Sie eine Eingabeaufforderung mit Administratorrechten öffnen und den folgenden Befehl eingeben:

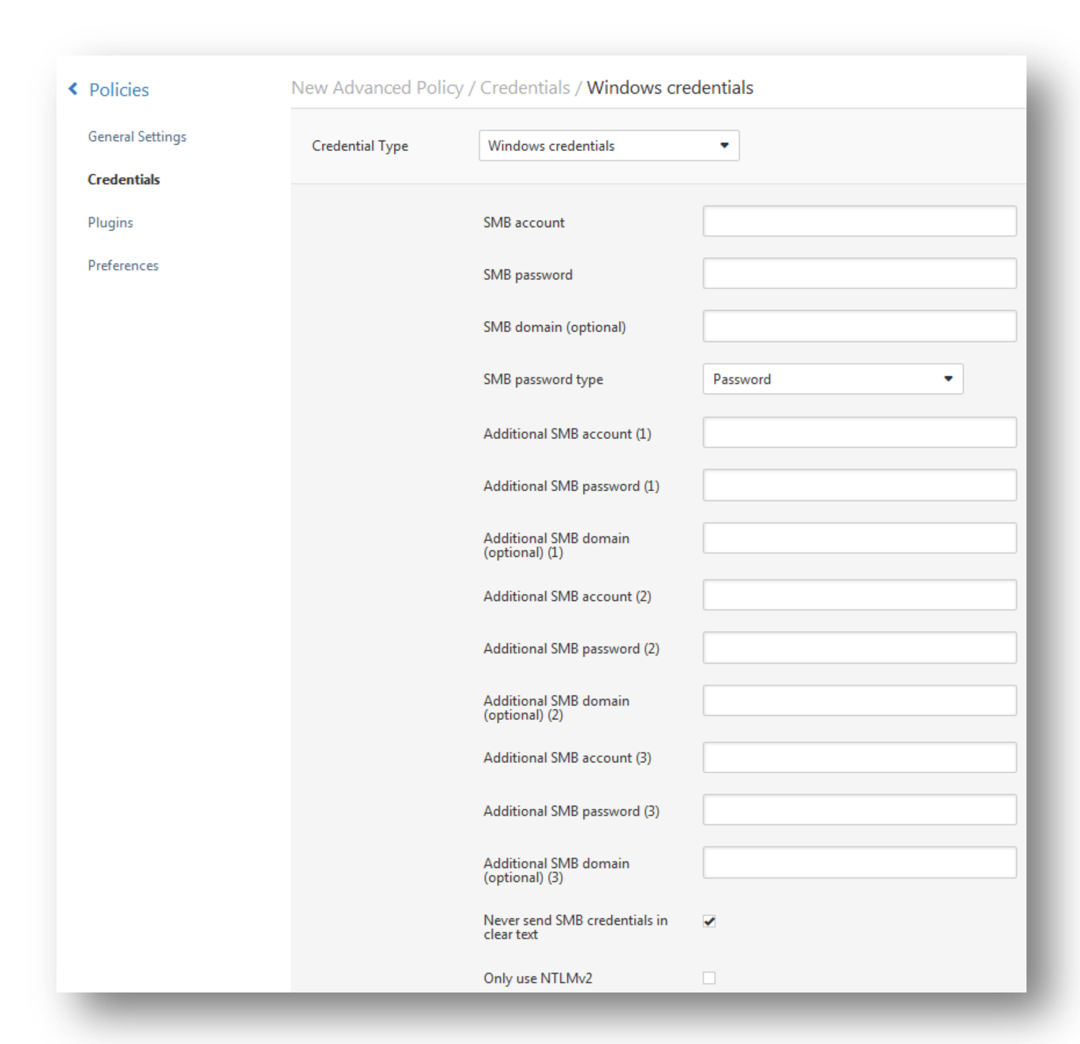
```
C:\> net user administrator /active:yes
```

Wenn ein SMB-Wartungskonto mit eingeschränkten Administratorrechten erstellt wird, kann Nessus mehrere Domänen einfach und sicher scannen.

Tenable empfiehlt Netzwerkadministratoren die Erstellung bestimmter Domänenkonten, um Tests zu vereinfachen. Nessus umfasst eine Vielzahl von Sicherheitstests für Windows NT, 2000, Server 2003, XP, Vista, Windows 7, Windows 8 und Windows 2008, die genauer arbeiten, wenn ein Domänenkonto angegeben wird. Allerdings versucht Nessus in den meisten Fällen, verschiedene Tests auch ohne Kontenangabe auszuführen.



Der Windows-Dienst „Remote-Registrierung“ ermöglicht Remotecomputern mit entsprechenden Anmeldedaten den Zugriff auf die Registrierung des überprüften Computers. Wird der Dienst nicht ausgeführt, dann ist das Auslesen von Schlüsseln und Werten aus der Registrierung auch bei Angabe gültiger Authentifizierungsdaten nicht möglich. Weitere Informationen entnehmen Sie dem Tenable-Blogbeitrag „Dynamic Remote Registry Auditing - Now you see it, now you don't!“. Dieser Dienst muss für einen authentifizierten Nessus-Scan ausgeführt werden, damit ein System unter Verwendung von Anmeldedaten vollständig geprüft werden kann.



Nach der Auswahl von „**SSH settings**“ („SSH-Einstellungen“) aus dem Dropdownmenü und der Eingabe von Anmeldedaten können UNIX-Systeme ausgewählt werden. Diese Anmeldedaten werden verwendet, um für Patchaudits oder Compliancetests lokale Informationen von UNIX-Remotesystemen abzurufen. Es sind Felder für die Eingabe des SSH-Benutzernamens für das Konto, unter dem die Tests auf dem UNIX-Zielsystem ausgeführt werden, sowie für das

SSH-Kennwort oder das SSH-Schlüsselpaar (öffentlicher und geheimer Schlüssel) vorhanden. In ein weiteres Feld können Sie ggf. die Passphrase für den SSH-Schlüssel eingeben.



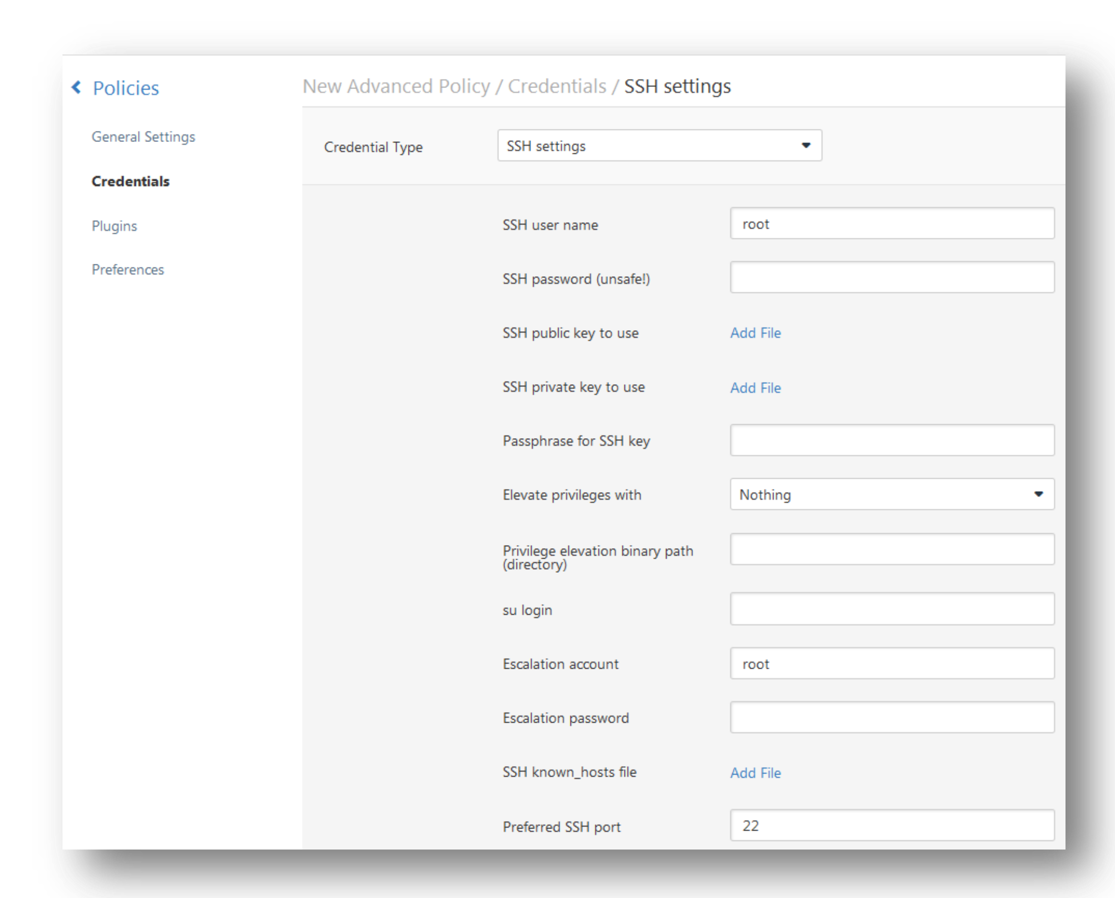
Nessus unterstützt die Verschlüsselungsalgorithmen `blowfish-cbc`, `aes-cbc` und `aes-ctr`.

Die wirksamsten authentifizierten Scans sind solche, bei denen das angegebene Konto über Root-Berechtigungen verfügt. Da zahlreiche Standorte eine Remoteanmeldung als Root nicht zulassen, können Nessus-Benutzer „**su**“, „**sudo**“, „**su+sudo**“, „**dzdo**“ oder „**pbrun**“ mit einem separaten Kennwort für ein Konto aufrufen, für das „**su**“- oder „**sudo**“-Berechtigungen konfiguriert wurden. Außerdem kann Nessus Berechtigungen auf Cisco-Geräten eskalieren, wenn „**Cisco 'enable'**“ ausgewählt wird.

Nessus kann zur Authentifizierung bei einem Remoteserver einen Zugriff auf SSH-Basis verwenden. Wenn die SSH-Datei **known_hosts** vorhanden und als Teil der Scanrichtlinie angegeben ist, wird Nessus sich, sofern möglich, nur bei den in dieser Datei genannten Hosts anmelden. Schließlich kann unter „Preferred SSH port“ noch der bevorzugte SSH-Port festgelegt werden, falls Nessus die Verbindung mit SSH über einen anderen als den Standardport 22 herstellen soll.

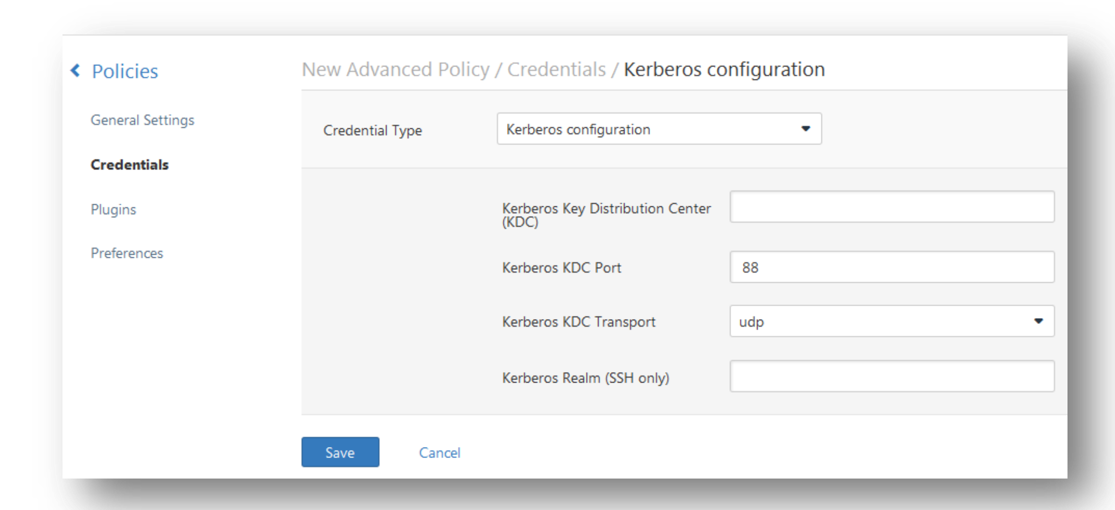
Nessus verschlüsselt alle in den Richtlinien gespeicherten Kennwörter. Allerdings wird empfohlen, zur Authentifizierung SSH-Schlüssel anstelle von SSH-Kennwörtern zu verwenden. Auf diese Weise soll sichergestellt werden, dass mithilfe des Benutzernamens und des Kennworts, die Sie für Audits Ihrer bekannten SSH-Server verwenden, kein Anmeldeversuch auf einem System vorgenommen wird, das sich nicht unter ihrer Kontrolle befindet. Aufgrund dessen wird zur Verwendung von SSH-Kennwörtern nur dann geraten, wenn es absolut unabdingbar ist.

Die folgende Bildschirmabbildung zeigt die verfügbaren SSH-Optionen. Das Dropdownmenü „Elevate privileges with“ („Berechtigungen hochstufen mit“) enthält verschiedene Methoden zum Hochstufen von Berechtigungen nach erfolgreicher Authentifizierung.

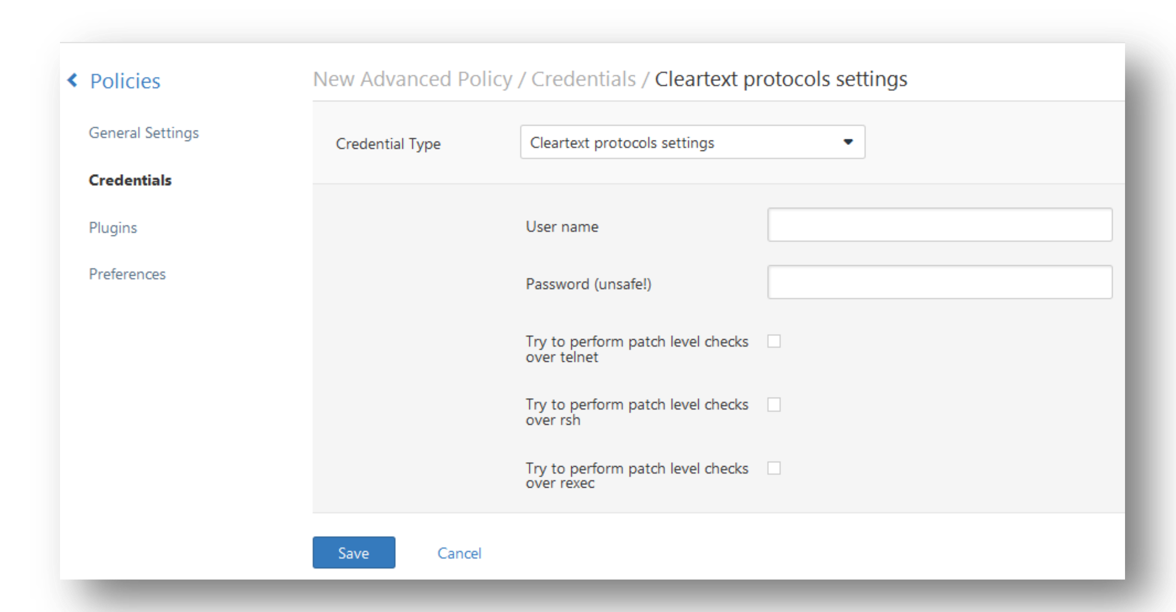


Wenn zur Eskalation von Berechtigungen ein anderes Konto als `root` verwendet werden muss, kann dieses unter „**Escalation account**" („Eskalationskonto") und das zugehörige Kennwort unter „**Escalation password**" („Eskalationskennwort") angegeben werden.

Mit „**Kerberos configuration**" („Kerberos-Konfiguration") können Sie Anmeldedaten unter Verwendung von Kerberos-Schlüsseln von einem Remotesystem aus angeben:



Schließlich kann, wenn eine sichere Methode zur Durchführung authentifizierter Tests nicht verfügbar ist, der Versuch erzwungen werden, Nessus-Tests über unsichere Protokolle durchzuführen. Hierzu muss das Element „**Cleartext protocol settings**" („Einstellungen für unverschlüsselte Protokolle") im Dropdownmenü konfiguriert werden. Unterstützt werden für diese Option die unverschlüsselten Protokolle **telnet**, **rsh** und **rexec**. Darüber hinaus können Sie mithilfe der Kontrollkästchen festlegen, dass Nessus Tests auf Patchebene über unverschlüsselte Protokolle durchführt:



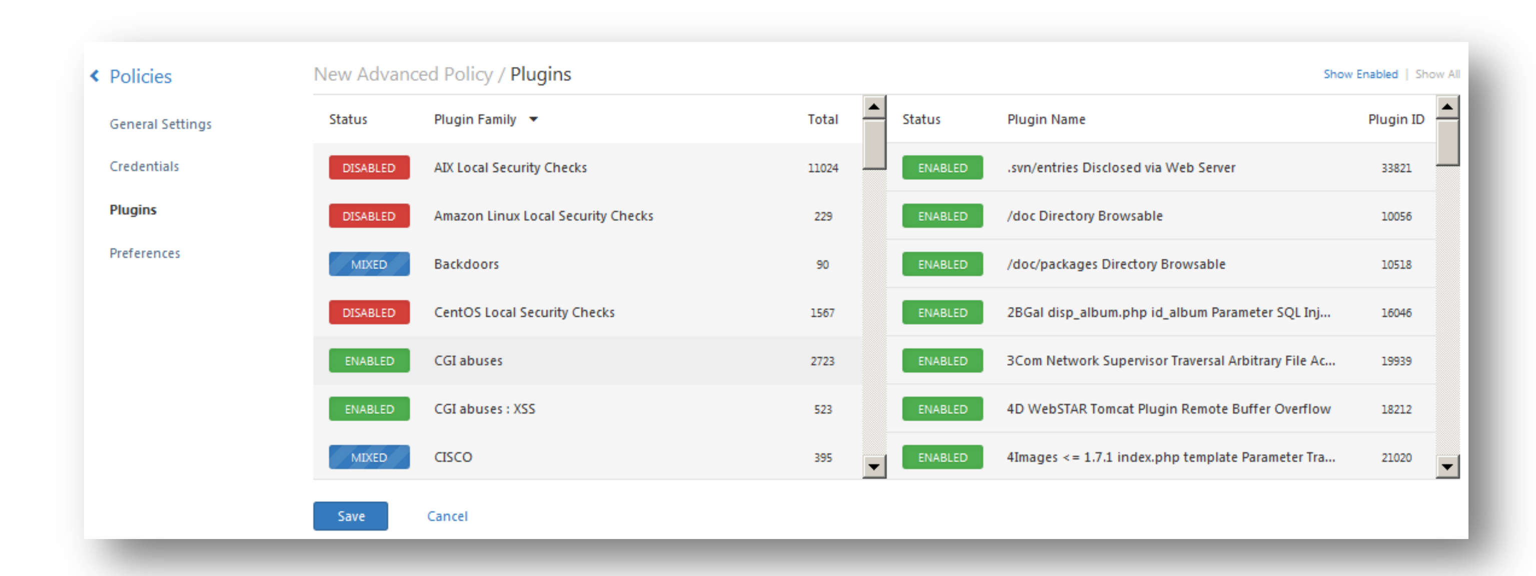
Standardmäßig sind alle Kennwörter (und auch die Richtlinie selbst) verschlüsselt. Wird die Richtlinie in einer **`.nessus`**-Datei gespeichert und diese **`.nessus`**-Datei nachfolgend auf eine andere Nessus-Installation kopiert, dann sind die Kennwörter für den zweiten Nessus-Scanner unzugänglich, da er sie nicht entschlüsseln kann.



Von der Verwendung unverschlüsselter Authentifizierungsdaten wird dringend abgeraten! Werden die Anmeldedaten remote (z. B. bei einem Nessus-Scan) übermittelt, dann können sie von jeder Person abgefangen werden, die Zugriff auf das Netzwerk hat. Deswegen sollten Sie, sofern dies irgendwie möglich ist, Mechanismen zur verschlüsselten Authentifizierung verwenden.

Plugins

Die Registerkarte „**Plugins**" ermöglicht die Auswahl bestimmter Sicherheitstests durch Plugin-Familien wie auch einzelne Tests.



Durch Anklicken der Plugin-Familie können Sie die gesamte Familie aktivieren (grün) oder deaktivieren (rot). Bei Auswahl einer Familie wird die Liste der zugehörigen Plugins angezeigt. Einzelne Plugins können separat aktiviert oder deaktiviert werden, um die Scanrichtlinien exakt für den eigenen Bedarf maßzuschneidern. Plugin-Familien, bei denen einige Plugins deaktiviert wurden, werden blau und mit dem Hinweis „mixed“ („gemischt“) angezeigt, um auf diesen Umstand hinzuweisen. Durch Anklicken der Plugin-Familie wird die gesamte Liste der Plugins geladen. Sie können dann abhängig von Ihren Scananforderungen eine passende Auswahl treffen.

Bei Auswahl eines Plugins wird dessen Ausgabe so angezeigt, wie sie später in einem Bericht enthalten sein wird. Die Zusammenfassung und die Beschreibung enthalten weitere Details zur untersuchten Sicherheitslücke. Wenn Sie im Browser nach unten blättern, werden außerdem Lösungsinformationen, zusätzliche Referenzen (falls vorhanden), Hinweise zu Risiken und Exploits sowie ggf. vorhandene Verweise auf Datenbanken mit Sicherheitslücken oder hilfreichen Angaben angezeigt.

New Advanced Policy / Plugins

Adobe ColdFusion Admin Requires No Authentication

Synopsis

ColdFusion administration does not require authentication.

Description

The remote web server is running ColdFusion, and Nessus was able to access its administration pages without authentication.

Solution

Configure ColdFusion administration to require authentication. This setting may be found in the ColdFusion administration menu under ' Security ' .

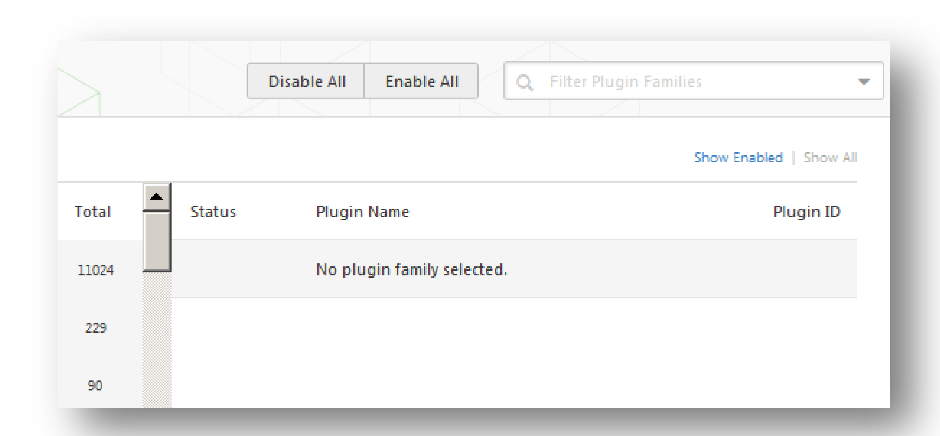
See Also

http://www.adobe.com/products/coldfusion/

Plugin Information

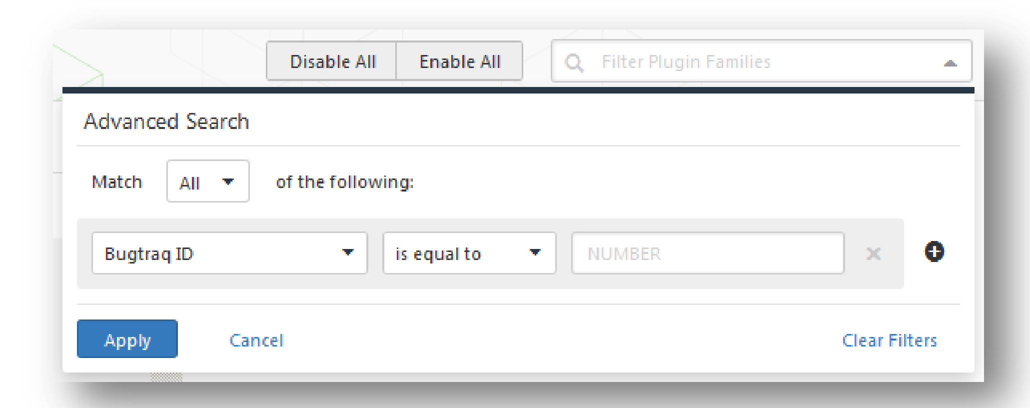
Plugin ID: 53297
Plugin Version: $Revision: 1.2 $

Oben auf der Seite mit den Plugin-Familien können Sie Filter einrichten, um eine Liste der Plugins zusammenzustellen, die in die Richtlinie aufgenommen werden, und alle Plugins zu aktivieren oder zu deaktivieren. Filter ermöglichen eine fein abgestufte Plugin-Auswahl. Für eine Richtlinie können mehrere Filter festgelegt sein.

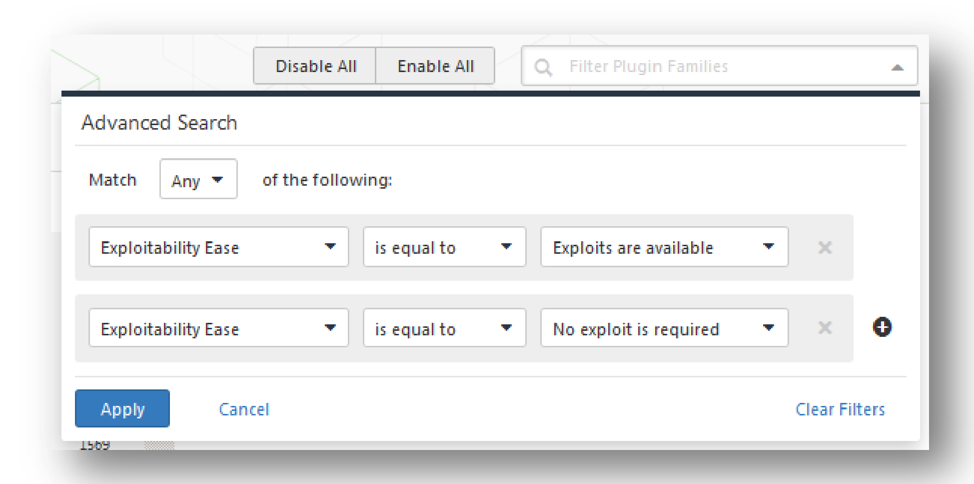


Wenn Sie nach Plugins suchen oder mehr über ein bestimmtes Plugin erfahren möchten, füllen Sie das Suchfeld aus, um Plugins unkompliziert nach ihrem Namen zu filtern. Die Plugins werden so in Echtzeit gefiltert. Anstelle eines Textes

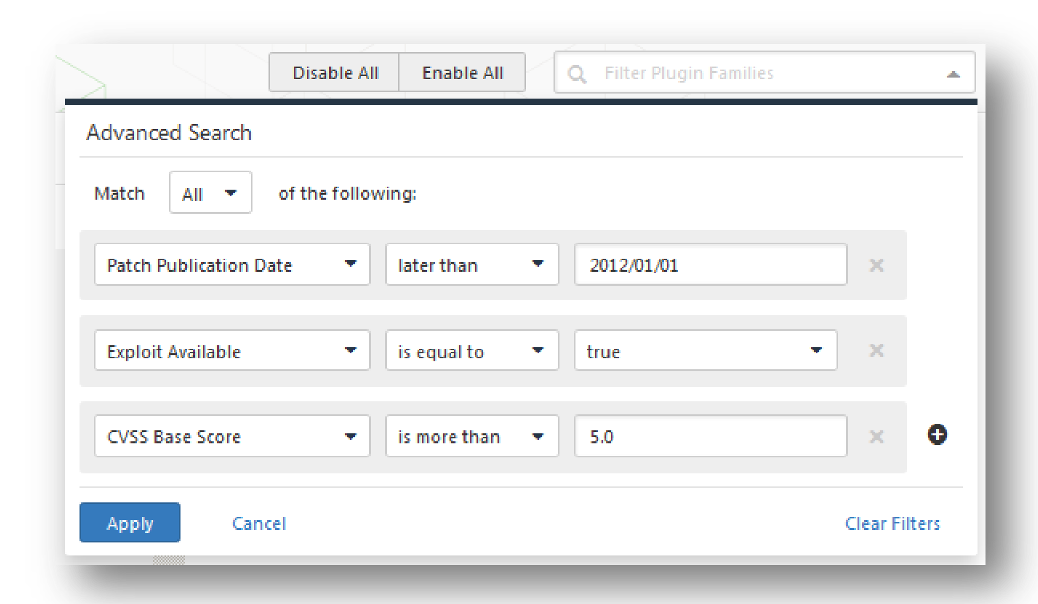
können Sie zum schnellen Suchen nach einem Plugin beispielsweise auch `id:10123` eingeben. Klicken Sie zum Erstellen eines Filters auf „**Filter Options**“ („Filteroptionen“):



Jeder Filter bietet Ihnen verschiedene Optionen, um die Suche zu verfeinern. Für die Anwendung der Filterkriterien stehen Ihnen die Optionen „Any“ („Beliebige“), bei der bereits bei Erfüllung mindestens eines Kriteriums ein Ergebnis zurückgegeben wird, und „All“ („Alle“) zur Verfügung, bei der alle Filterkriterien vorhanden sein müssen. Wenn Sie beispielsweise eine Richtlinie nur mit solchen Plugins erstellen möchten, für die ein Exploit vorhanden ist **oder** die ohne Skript-Exploit genutzt werden können, erstellen Sie drei Filter und wählen als Kriterium „Any“ aus:



Möchten Sie eine Richtlinie mit Plugins erstellen, die mehreren Kriterien entsprechen, dann wählen Sie „All“ aus und fügen die gewünschten Filter hinzu. Die nachfolgende Richtlinie beispielsweise würde alle nach dem 1. Januar 2012 veröffentlichten Plugins enthalten, für die ein öffentlicher Exploit vorhanden ist und die eine CVSS-Basisbewertung von mehr als 5.0 aufweisen:



Eine vollständige Liste der Filterkriterien und zugehörigen Parameter finden Sie im Abschnitt „Berichtfilter“ des vorliegenden Dokuments.



Zur Erstellung von Richtlinien mithilfe von Filtern wird empfohlen, zunächst alle Plugins zu deaktivieren. Ermitteln Sie die Plugins, die Bestandteil der Richtlinie werden sollen, dann mithilfe von Plugin-Filtern. Wenn Sie fertig sind, wählen Sie die einzelnen Plugin-Familien aus und klicken auf „Enable Plugins“ („Plugins aktivieren“).

Wenn eine Richtlinie erstellt und gespeichert wird, sind in ihr alle Plugins vermerkt, die ursprünglich ausgewählt wurden. Wenn neue Plugins über ein Plugin-Update empfangen werden, werden diese automatisch aktiviert, sofern die zugehörige Familie in der Richtlinie bereits aktiviert ist. Wurde die Familie vollständig oder teilweise deaktiviert, dann werden auch neue Plugins dieser Familie automatisch deaktiviert.



Die Familie „Denial of Service“ enthält einige Plugins, die in einem Netzwerk Ausfälle verursachen können, wenn die Option „Safe Checks“ deaktiviert ist; auf der anderen Seite enthält sie auch einige nützliche Tests, die keinen Schaden anrichten können. Sie können die Familie „Denial of Service“ in Verbindung mit der aktivierten Option „Safe Checks“ verwenden, um sicherzustellen, dass potenziell gefährliche Plugins nicht ausgeführt werden. Es empfiehlt sich jedoch, die Familie „Denial of Service“ nur dann in einem Produktionsnetzwerk einzusetzen, wenn der Einsatz für ein Wartungsfenster geplant werden kann und Personal zur Fehlerbehebung bereitsteht.

Preferences

Die Registerkarte „**Preferences**“ („Voreinstellungen“) enthält Optionen für eine fein abgestufte Steuerung der Scanrichtlinieneinstellungen. Bei Auswahl eines Elements aus dem Dropdownmenü werden weitere Konfigurationselemente für die betreffende Kategorie angezeigt. Beachten Sie, dass die Liste der Konfigurationsoptionen dynamisch ist, d. h., sie hängt von der Nessus-Version, von den Auditrichtlinien und weiteren Funktionen ab, auf die der verbundene Nessus-Scanner zugreifen kann. Kostenpflichtige Nessus-Versionen verfügen unter Umständen über

anspruchsvollere Konfigurationsoptionen als Nessus Home. Außerdem ändert sich diese Liste, wenn Plugins hinzugefügt oder geändert werden.

Die folgende Liste bietet eine Übersicht über alle Einstellungen. Ausführlichere Informationen zu den einzelnen Parametern entnehmen Sie dem Abschnitt „Scanvoreinstellungen im Detail" im vorliegenden Dokument.

Einstellung	Beschreibung
ADSI settings (ADSI-Einstellungen)	Mit ADSI (Active Directory Service Interfaces) werden Informationen zu Android- und iOS-Geräten vom MDM-Server (Mobile Device Management) abgerufen.
Apple Profile Manager API Settings (API-Einstellungen des Apple Profil-Managers)	Option der kostenpflichtigen Version zur Aktivierung von Enumeration und Sicherheitslückenscans auf Geräten unter Apple iOS wie iPhone, iPad usw.
Cisco IOS Compliance Checks (Cisco IOS-Compliancetests)	Option der kostenpflichtigen Version, die die Angabe einer Richtliniendatei zum Testen von Cisco IOS-Geräten auf die Einhaltung von Compliancestandards gestattet
Database Compliance Checks (Datenbank-Compliancetests)	Option der kostenpflichtigen Version, die die Angabe einer Richtliniendatei zum Testen von Datenbanken wie DB2, SQL Server, MySQL und Oracle auf die Einhaltung von Compliancestandards gestattet
Database Settings (Datenbankeinstellungen)	Optionen zur Angabe des zu testenden Datenbanktyps und der zu verwendenden Anmeldedaten
Do not scan fragile devices (Anfällige Geräte nicht scannen)	Mithilfe dieser Optionen weisen Sie Nessus an, bestimmte Geräte **nicht** zu scannen, weil ein erhöhtes Risiko besteht, die Zielgeräte zum Absturz zu bringen.
Global variable settings (Einstellungen globaler Variablen)	Zahlreiche Optionen für die Nessus-Konfiguration
HTTP cookies import (HTTP-Cookies importieren)	Beim Testen von Webanwendungen wird mit dieser Option eine externe Datei angegeben, in die HTTP-Cookies importiert werden, um eine Authentifizierung bei der Anwendung zu gestatten.
HTTP login page (HTTP-Anmeldeseite)	Einstellungen, die sich auf die Anmeldeseite bei Webanwendungstests beziehen
IBM iSeries Compliance Checks (Compliancetests für IBM iSeries-Systeme)	Option der kostenpflichtigen Version, die die Angabe einer Richtliniendatei zum Testen von IBM iSeries-Systemen auf die Einhaltung von Compliancestandards gestattet
IBM iSeries Credentials (Anmeldedaten für IBM iSeries)	Bezeichnet den Speicherort der Anmeldedaten für IBM iSeries-Systeme.
ICCP/COTP TSAP Addressing Weakness (Schwächen bei der ICCP/COTP-TSAP-Adressierung)	Option der kostenpflichtigen Version für SCADA-Tests (Supervisory Control And Data Acquisition)
Login configurations (Anmeldekonfigurationen)	Bezeichnet den Speicherort, an dem Anmeldedaten für einfache HTTP-, NNTP-, FTP-, POP- und IMAP-Diensttests abgelegt sind.

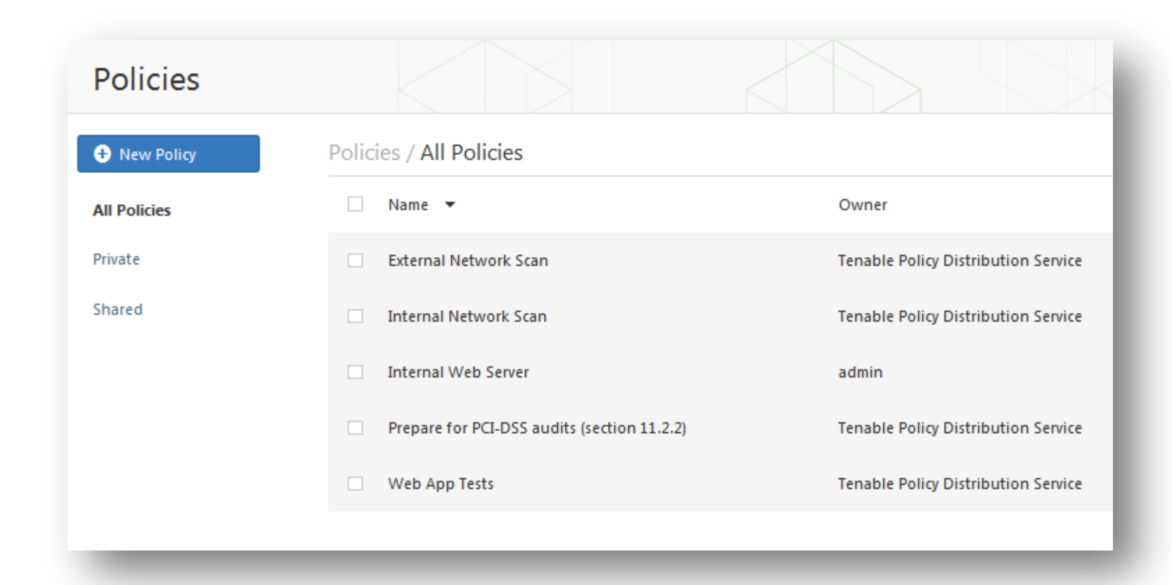
Modbus/TCP Coil Access (Modbus/TCP Coil-Zugriff)	Option der kostenpflichtigen Version für SCADA-Tests (Supervisory Control And Data Acquisition)
Nessus SYN scanner (Nessus SYN-Scanner)	Optionen für den integrierten SYN-Scanner
Nessus TCP scanner (Nessus TCP-Scanner)	Optionen für den integrierten TCP-Scanner
News Server (NNTP) Information Disclosure (NNTP-Datenpreisgabe)	Optionen zum Testen von NNTP-Servern auf bestimmte Sicherheitslücken, durch die Daten preisgegeben werden könnten
Oracle Settings (Oracle-Einstellungen)	Optionen für Tests von Oracle-Datenbankinstallationen
PCI DSS Compliance (PCI-DSS-Compliance)	Option der kostenpflichtigen Version, mit der Nessus angewiesen wird, Scanergebnisse mit PCI-DSS-Standards zu vergleichen.
Patch Management: Red Hat Satellite Server Settings (Patchmanagement: Einstellungen für Red Hat-Satellite-Server)	Optionen für die Integration von Nessus mit dem Red Hat-Satellite-Patchmanagementserver. Weitere Informationen entnehmen Sie dem Dokument „Patch Management Integration" („Integration des Patchmanagements").
Patch Management: SCCM Server Settings (Patchmanagement: Einstellungen für SCCM-Server)	Optionen für die Integration von Nessus mit dem SCCM-Patchmanagementserver (System Center Configuration Manager). Weitere Informationen entnehmen Sie dem Dokument „Patch Management Integration" („Integration des Patchmanagements").
Patch Management: VMware Go Server Settings (Patchmanagement: Einstellungen für VMware Go Server)	Optionen für die Integration von Nessus mit dem VMware Go Server (vormals Shavlik). Weitere Informationen entnehmen Sie dem Dokument „Patch Management Integration" („Integration des Patchmanagements").
Patch Management: WSUS Server Settings (Patchmanagement: Einstellungen für WSUS-Server)	Optionen für die Integration von Nessus mit dem WSUS-Patchmanagementserver (Windows Server Update Service). Weitere Informationen entnehmen Sie dem Dokument „Patch Management Integration" („Integration des Patchmanagements").
Ping the remote host (Pingbefehl an Remotehost senden)	Mit diesen Einstellungen steuert Nessus die Ping-basierte Netzwerkerkennung.
Port scanner settings (Einstellungen für Portscanner)	Zwei Einstellungen, die die Steuerung von Portscanaktivitäten verbessern
SMB Registry: Start the Registry Service during the scan (SMB-Registrierung: Registrierungsdienst bei laufendem Scan starten)	Hiermit wird Nessus angewiesen, den SMB-Registrierungsdienst auf Hosts zu starten, auf denen er nicht aktiviert ist.

SMB Scope (SMB-Umfang)	Hiermit wird Nessus angewiesen, Domänenbenutzer anstelle lokaler Benutzer abzufragen.
SMB Use Domain SID to Enumerate Users (SMB: Domänen-SID für Benutzerenumeration verwenden)	Mit dieser Option können Sie den SID-Bereich für SMB-Lookups von Domänenbenutzern angeben.
SMB Use Host SID to Enumerate Local Users (SMB: Host-SID für Enumeration lokaler Benutzer verwenden)	Mit dieser Option können Sie den SID-Bereich für SMB-Lookups lokaler Benutzer angeben.
SMTP Settings (SMTP-Einstellungen)	Optionen für SMTP-Tests (Simple Mail Transport Protocol)
SNMP Settings (SNMP-Einstellungen)	Konfigurations- und Authentifizierungsdaten für SNMP (Simple Network Management Protocol)
Service Detection (Diensterkennung)	Mit diesen Optionen werden Tests SSL-basierter Dienste gesteuert.
Unix Compliance Checks (UNIX-Compliancetests)	Option der kostenpflichtigen Version, die die Angabe einer Richtliniendatei zum Testen von UNIX-Systemen auf die Einhaltung von Compliancestandards gestattet
VMware SOAP API Settings (Einstellungen für VMware-SOAP-API)	Konfigurations- und Authentifizierungsdaten für die SOAP-API von VMware
Wake-on-LAN (WOL)	Hiermit wird Nessus angewiesen, vor der Durchführung eines Scans Wake-on-LAN-Pakete zu senden.
Web Application Test Settings (Einstellungen für Webanwendungstests)	Optionen für Tests von Webanwendungen
Web mirroring (Webspiegelung)	Konfigurationsdetails zur Steuerung der Anzahl von Webseiten, die von Nessus gespiegelt werden, um die Inhalte auf Sicherheitslücken zu prüfen
Windows Compliance Checks (Windows-Compliancetests)	Option der kostenpflichtigen Version, die die Angabe einer Richtliniendatei zum Testen von Windows-Systemen auf die Einhaltung von Compliancestandards gestattet
Windows File Contents Compliance Checks (Compliancetests für Windows-Dateiinhalte)	Option der kostenpflichtigen Version, die die Angabe einer Richtliniendatei zum Testen von Dateien auf Windows-Systemen auf die Einhaltung von Compliancestandards gestattet



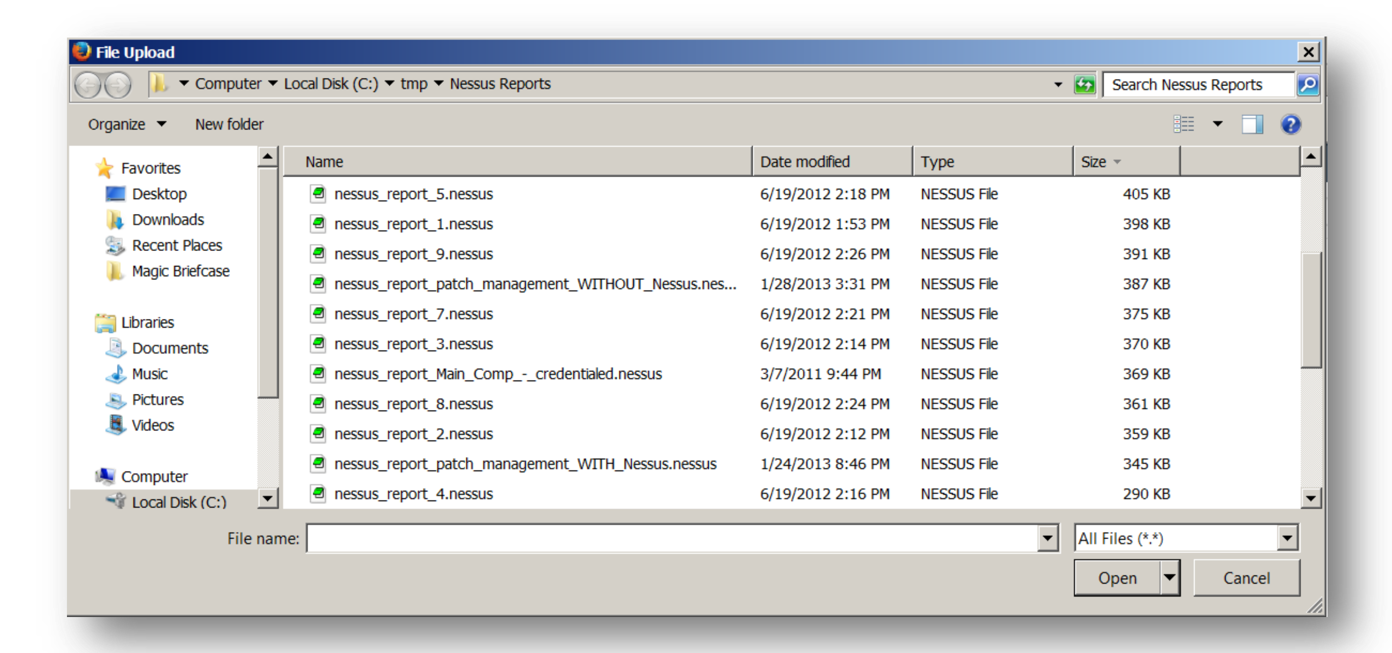
Aufgrund aktualisierter XML-Metadaten in Nessus 5 stehen mit Nessus 4 generierte Compliancedaten im Abschnitt „Compliance Checks“ exportierter Berichte nicht mehr zur Verfügung. Allerdings sind die Compliancedaten über die Nessus-Benutzeroberfläche ersichtlich.

Zur praktischen Nutzung bietet Nessus auf der linken Seite zwei Filtervoreinstellungen für private („Private“) und gemeinsam verwendete Richtlinien („Shared“):



Richtlinien importieren, exportieren und kopieren

Über die Schaltfläche „**Upload**“ in der Menüleiste können Sie zuvor erstellte Richtlinien in den Scanner hochladen. Wählen Sie im Dialogfeld „Durchsuchen…“ die Richtlinie auf Ihrem lokalen System aus und klicken Sie auf „**Öffnen**“.



Über die Schaltfläche „**Options**“ („Optionen“) in der Menüleiste können Sie die betreffende Richtlinie aus dem Scanner in das lokale Dateisystem herunterladen. Im Downloaddialogfeld des Browsers können Sie angeben, dass die Richtlinie in einem externen Programm (z. B. dem Texteditor) geöffnet oder in einem frei wählbaren Verzeichnis gespeichert wird.

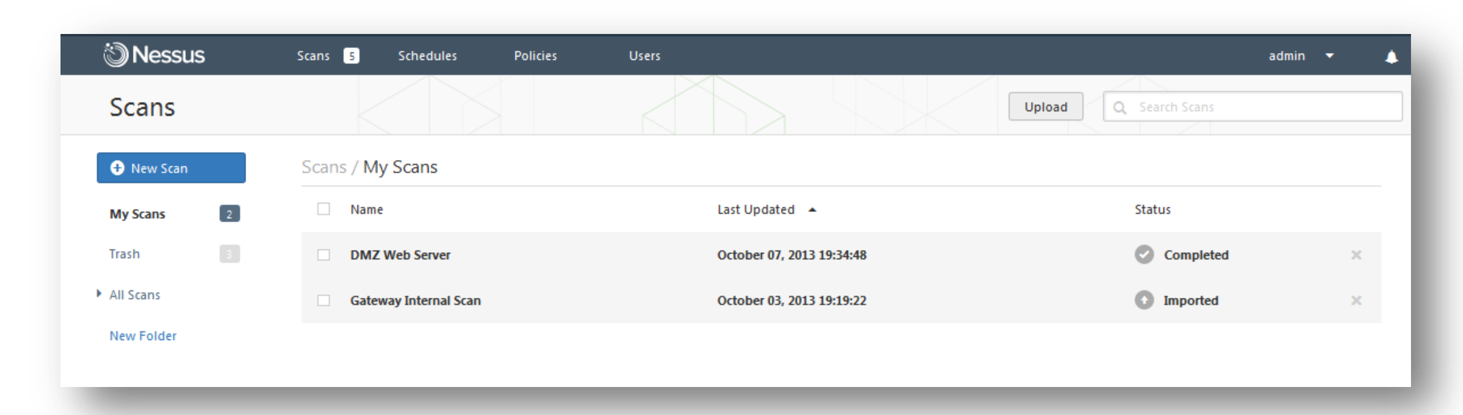


Kennwörter und `.audit`-Dateien, die in einer Richtlinie enthalten sind, werden nicht exportiert.

Wenn Sie eine Richtlinie erstellen möchten, die im Vergleich zu einer vorhandenen Richtlinie nur kleinere Änderungen aufweist, können Sie die Ausgangsrichtlinie in der Liste auswählen und dann in der Menüleiste auf „**Options**“ und dann auf „**Copy Policy**“ („Richtlinie kopieren“) klicken. Hierdurch wird eine Kopie der Ausgangsrichtlinie erstellt, die bearbeitet werden kann, um die erforderlichen Änderungen vorzunehmen. Dies ist sinnvoll zur Erstellung von Standardrichtlinien mit geringfügigen Änderungen, wie sie für die gegebene Umgebung erforderlich sind.

Scans erstellen, starten und planen

Benutzer können eigene Berichte erstellen, die verschiedene Kapitel enthalten. Diese heißen „Vulnerability Centric“ („Sicherheitslückenzentrisch“), „Host Centric“ („Hostzentrisch“), „Compliance“ und „Compliance Executive“. Das HTML-Format wird weiterhin als Standard unterstützt. Sofern Java jedoch auf dem Scannerhost installiert ist, ist es jetzt möglich, Berichte im PDF-Format zu exportieren. Mithilfe von Berichtsfiltern und Exportfunktionen kann der Benutzer dynamische Berichte auf der Basis der eigenen Prioritäten erstellen, statt lediglich aus einer Liste vorgefertigter Berichte auszuwählen.

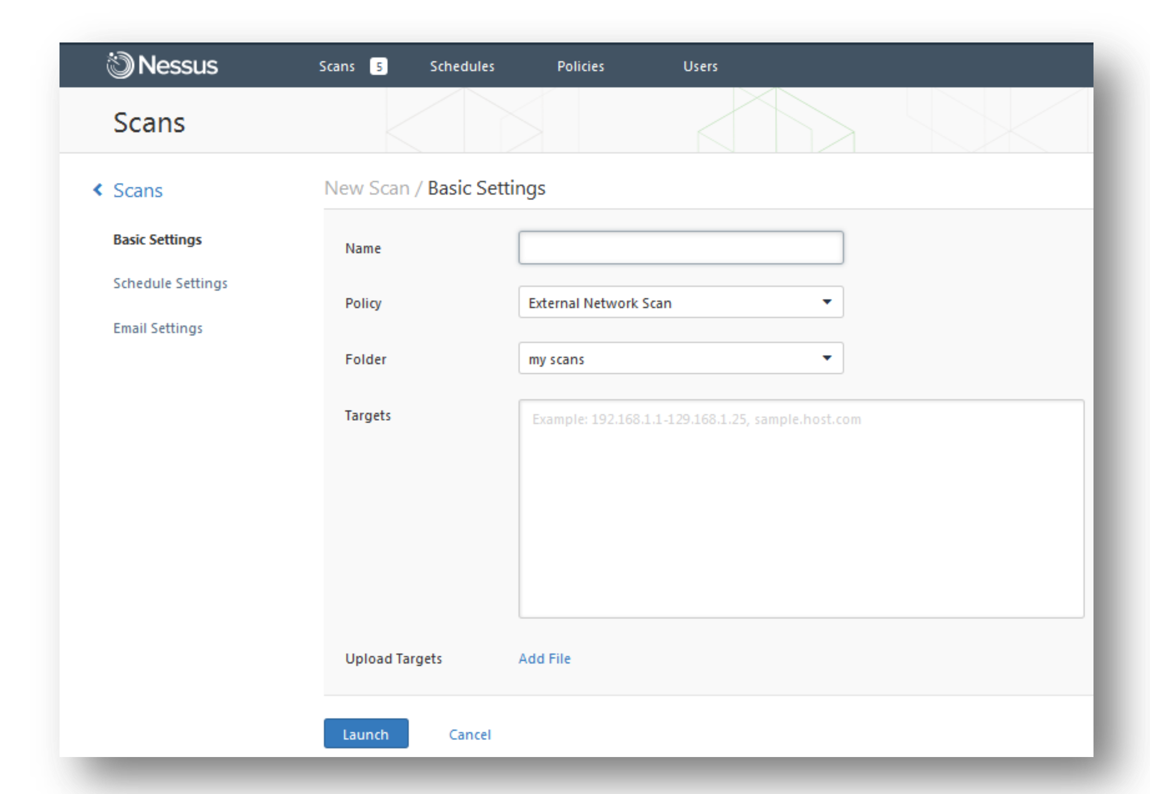


Folgende Scanstatusebenen stehen in der Scanlistentabelle bereit:

Scanstatus	Beschreibung
Completed (Abgeschlossen)	Der Scan wurde abgeschlossen.
Canceled (Vorzeitig beendet)	Der Benutzer hat den Scan vorzeitig beendet.
Aborted (Abgebrochen)	Der Scan wurde aufgrund einer ungültigen Zielliste oder eines Serverfehlers (z. B. infolge eines Neustarts oder Absturzes) abgebrochen.
Imported (Importiert)	Der Scan wurde mit der Upload-Funktion importiert.

Diese Statusebenen gelten ggf. nur für neue Scans. Alte Scans erhalten automatisch den Status „Completed“. Scans mit demselben Status können in den virtuellen Ordnern im linken Navigationsbereich aufgelistet werden.

Wenn Sie eine Richtlinie erstellt oder ausgewählt haben, können Sie einen neuen Scan anlegen. Klicken Sie hierzu auf die Option „**Scans**“ oben in der Menüleiste und dann rechts auf die Schaltfläche „**+ New Scan**“ („Neuer Scan“). Das Fenster „**New Scan**“ („Neuer Scan“) erscheint:



Auf der Registerkarte „**Basic Settings**“ („**Grundeinstellungen**“) sind fünf Felder zur Eingabe des Scanziels vorhanden:

- **Name.** Hier wird der Name festgelegt, der zur Bezeichnung des Scans auf der Nessus-Benutzeroberfläche verwendet wird.
- **Policy („Richtlinie“).** Wählen Sie eine zuvor erstellte Richtlinie aus, anhand derer die Parametereinstellungen für den Scan vorgenommen werden.
- **Folder („Ordner“).** Ordner auf der Nessus-Benutzeroberflächen, in dem die Scanergebnisse gespeichert werden
- **Scan Targets („Scanziele“).** Scanziele können als einzelne IP-Adresse (z. B. „192.168.0.1“), als IP-Bereich (z. B. „192.168.0.1-192.168.0.255“), als Subnetz in CIDR-Notation (z. B. „192.168.0.0/24“) oder als auflösbarer Host (z. B. „www.nessus.org“) angegeben werden.
- **Upload Targets („Uploadziele“).** Klicken Sie auf „**Add File**“ („Datei hinzufügen“) und wählen Sie auf dem lokalen Computer eine Textdatei aus, die eine Liste mit Hosts enthält.



Die Hostdatei muss im ASCII-Format vorliegen. Pro Zeile muss ein Host angegeben sein, und es dürfen weder Leerzeichen noch Leerzeilen vorhanden sein. Die Unicode-/UTF-8-Kodierung wird nicht unterstützt.

Beispiel für Hostdateiformate:

Einzelne Hosts:

192.168.0.100
192.168.0.101
192.168.0.102

Hostbereich:

192.168.0.100-192.168.0.102

Hostblock in CIDR-Notation:

192.168.0.1/24

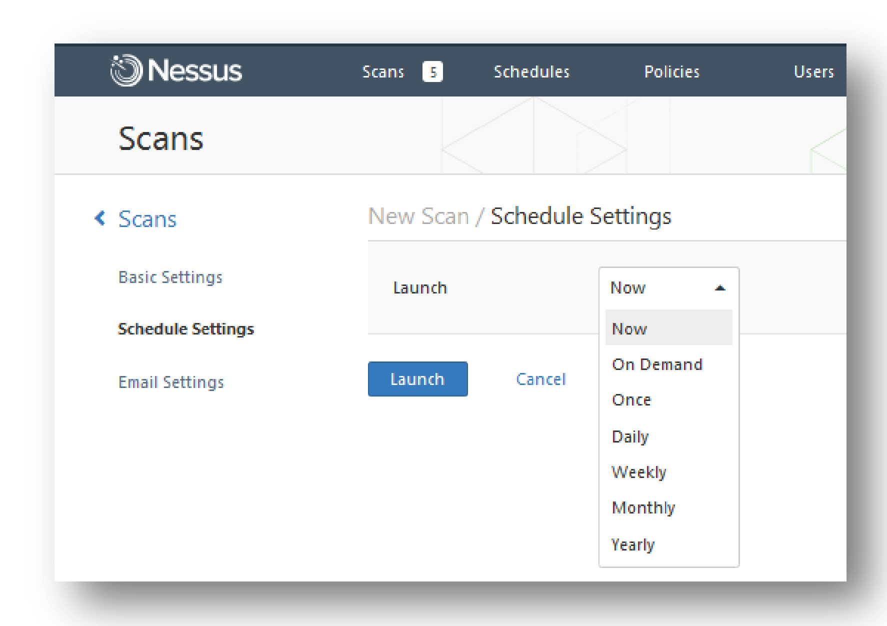
Virtuelle Server:

www.tenable.com[192.168.1.1]
www.nessus.org[192.168.1.1]
www.tenablesecurity.com[192.168.1.1]



Je nach Ihren Scaneinstellungen („**max hosts**", „**max checks per host**" usw.) kann hierdurch eine Drosselung der virtuellen Hosts hervorgerufen werden, da sie für Nessus dieselbe IP-Adresse aufweisen. Auf Nicht-Windows-Hosts können Nessus-Administratoren eine angepasste erweiterte Einstellung namens **`multi_scan_same_host`** hinzufügen und sie auf **`true`** setzen. Somit kann der Scanner mehrere Scans derselben IP-Adresse vornehmen. Beachten Sie, dass der PCAP-Treiber unter Windows dies unabhängig von der Nessus-Konfiguration nicht zulässt. Diese Funktion wird ab Nessus 5.2.0 angeboten.

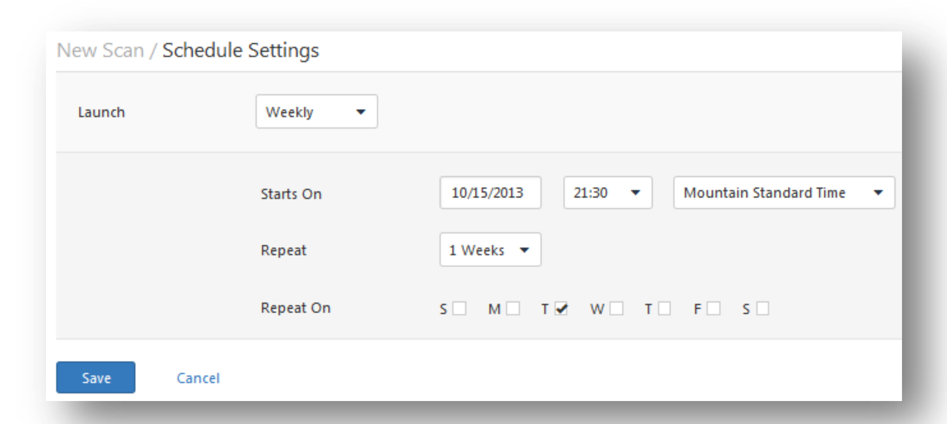
Im Register „**Schedule Settings**" („Einstellungen für die Zeitplanung") gibt es ein Dropdownmenü, das den Startzeitpunkt des Scans kontrolliert:



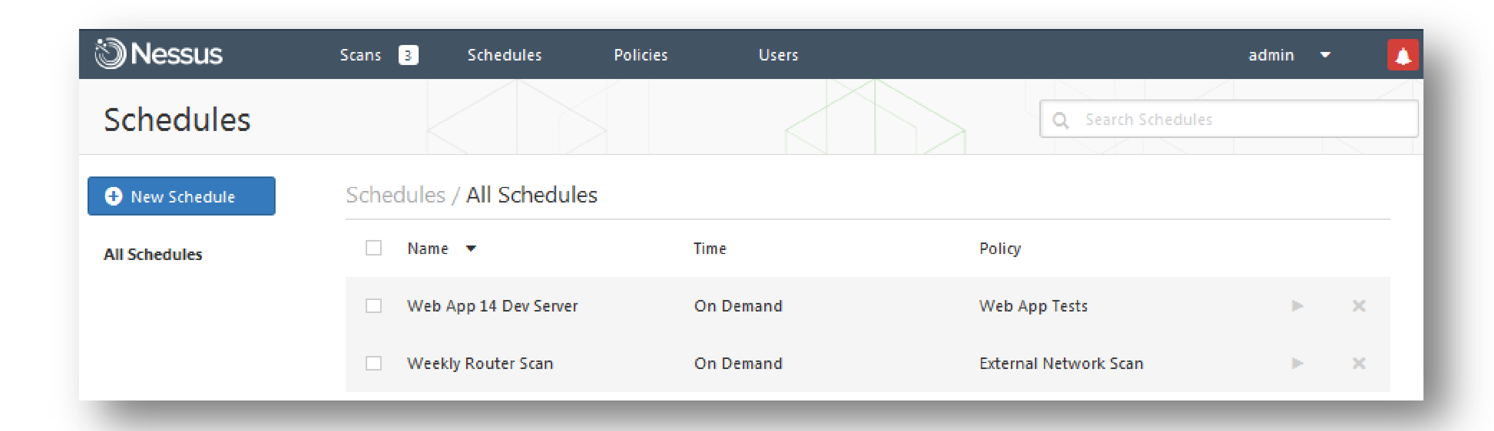
Die Startoptionen sind:

- **Now (Jetzt).** Sofort starten.
- **On Demand (Auf Abruf).** Der Scan wird als Vorlage eingerichtet, sodass er jederzeit manuell gestartet werden kann (dies entspricht der früheren Funktion „Scan Template“).
- **Once (Einmalig).** Der Scan wird für einen bestimmten Zeitpunkt geplant.
- **Daily (Täglich).** Der Scan soll für maximal 20 Tage täglich zu einer bestimmten Uhrzeit oder in bestimmten Abständen erfolgen.
- **Weekly (Wöchentlich).** Der Scan soll über maximal 20 Wochen an einem bestimmten Wochentag zu einer bestimmten Uhrzeit ausgeführt werden.
- **Monthly (Monatlich).** Der Scan soll über maximal 20 Monate an einem bestimmten Wochentag in einer bestimmten Woche zu einer bestimmten Uhrzeit ausgeführt werden.
- **Yearly (Jährlich).** Der Scan soll über maximal 20 Jahre jedes Jahr an einem bestimmten Tag und zu einer bestimmten Uhrzeit ausgeführt werden.

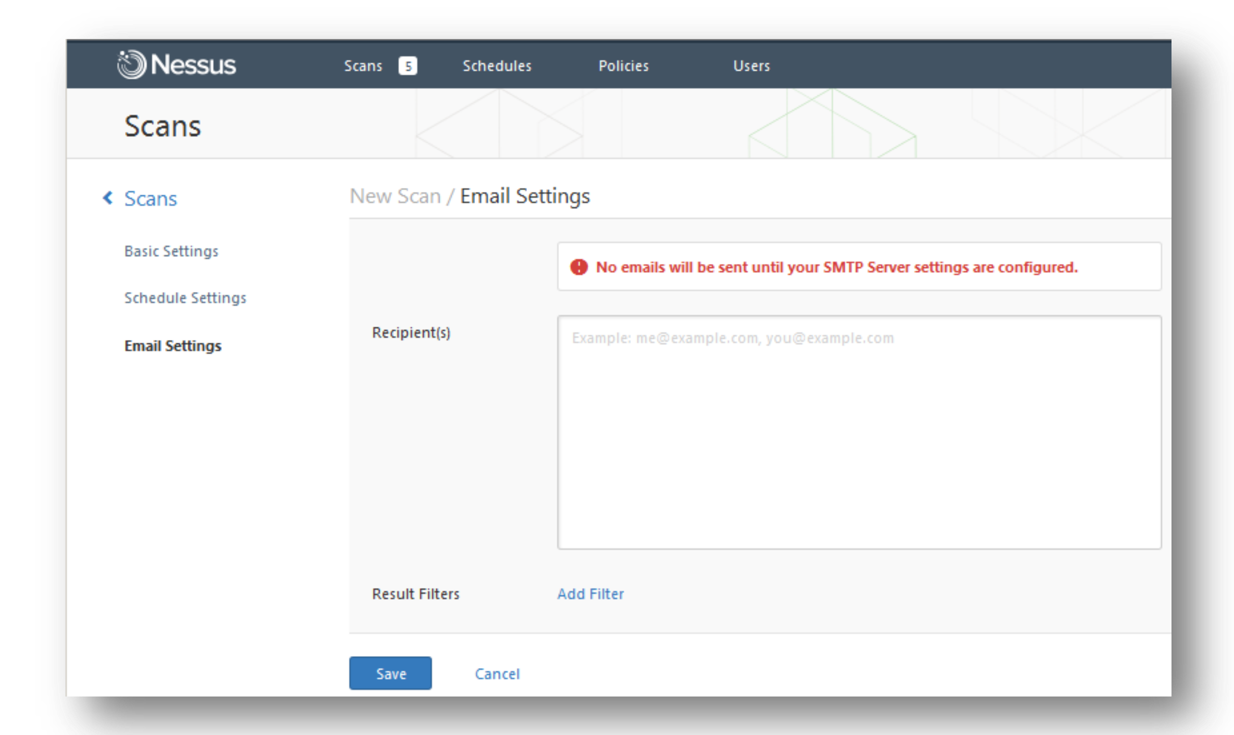
Es folgt ein Beispiel für einen geplanten Scan:



Nach Erstellung eines geplanten Scans können Sie über das oben gezeigte Menü „Schedules“ (Zeitpläne) darauf zugreifen. Diese Seite ermöglicht die Verwaltung von geplanten Scans und deren Aktualisierung bei Bedarf:

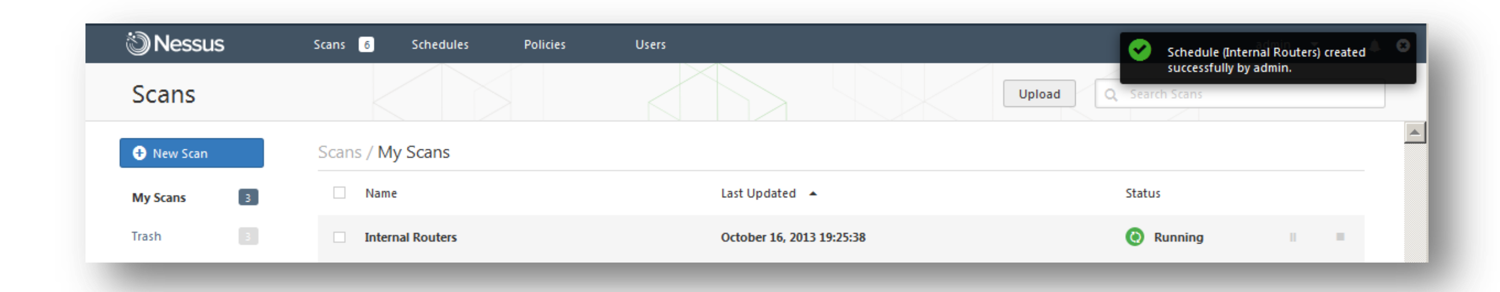


Auf der Registerkarte „**Email Settings**“ („E-Mail-Einstellungen“) können Sie E-Mail-Adressen konfigurieren, an die die Scanergebnisse nach Abschluss des Scans gesendet werden.

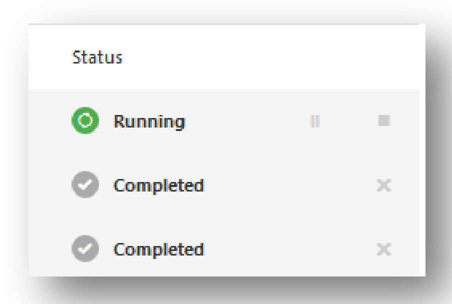


Die Funktion „**Email Scan Results**“ („Scanergebnisse per E-Mail senden“) erfordert die Konfiguration der SMTP-Einstellungen durch einen Nessus- Administrator. Weitere Informationen zur Konfiguration der SMTP-Einstellungen finden Sie im „Nessus 5.2-Installations- und Konfigurationshandbuch“. Wenn Sie diese Einstellungen noch nicht konfiguriert haben, weist Nessus Sie darauf hin, dass diese eingerichtet werden müssen, damit die Funktion verwendet werden kann.

Klicken Sie nach Eingabe der Scaninformationen auf „**Save**“ („Speichern“). Nach der Übertragung beginnt der Scan sofort, sofern Sie zuvor „**Now**“ („Jetzt“) ausgewählt haben. Erst nach Abschluss des Scans wird wieder die Seite „**Scans**“ angezeigt. In der oberen Menüleiste wird zudem die Anzahl der zurzeit ausgeführten Scans auf der Schaltfläche „**Scans**“ angezeigt.



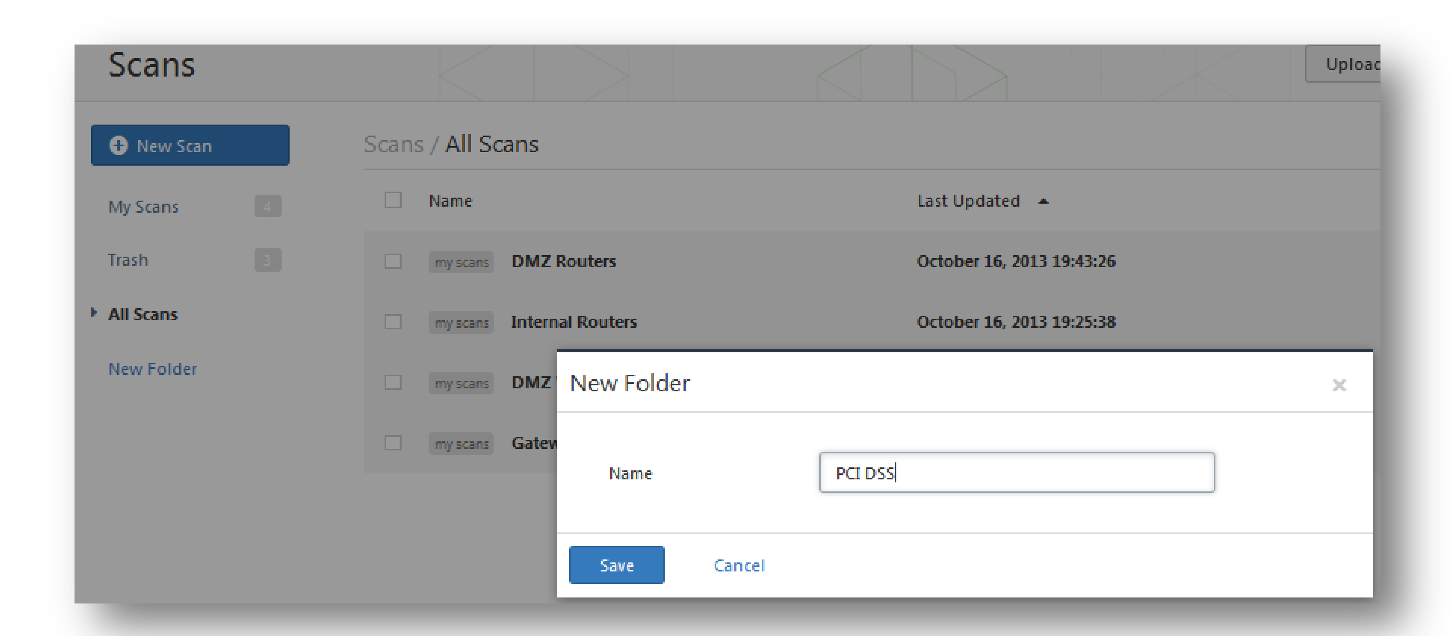
Nach dem Starten des Scans zeigt die Liste „**Scans**“ alle laufenden oder unterbrochenen Scans sowie grundlegende Informationen zum Scan an. Auf der linken Seite erscheinen bei laufendem Scan die Schaltflächen „Pause“ und „Stop“, mit denen der Status geändert werden kann:



Wenn Sie einen bestimmten Scan durch Aktivieren des Kontrollkästchens auf der linken Seite aus der Liste ausgewählt haben, können Sie über die Schaltflächen „**More**“ („Mehr“) und „**Move To**“ („Verschieben nach“) weitere Bedienschritte auswählen. Hierzu gehören das Umbenennen des Scans, das Ändern des Scanstatus, das Markieren als gelesen und das Verschieben in einen anderen Ordner.

Scanergebnisse durchsuchen

Scans lassen sich in Ordnern ablegen. Links finden Sie die beiden Standardordner „My Scans“ („Eigene Scans“) und „Trash“ („Papierkorb“). Alle neuen Scans werden standardmäßig im virtuellen Ordner „**My Scans**“ abgelegt. Die Standardablage für neue Scans kann geändert werden. Zum Erstellen neuer Ordner rufen Sie die Funktion „**New Folder**“ („**Neuer Ordner**“) auf:

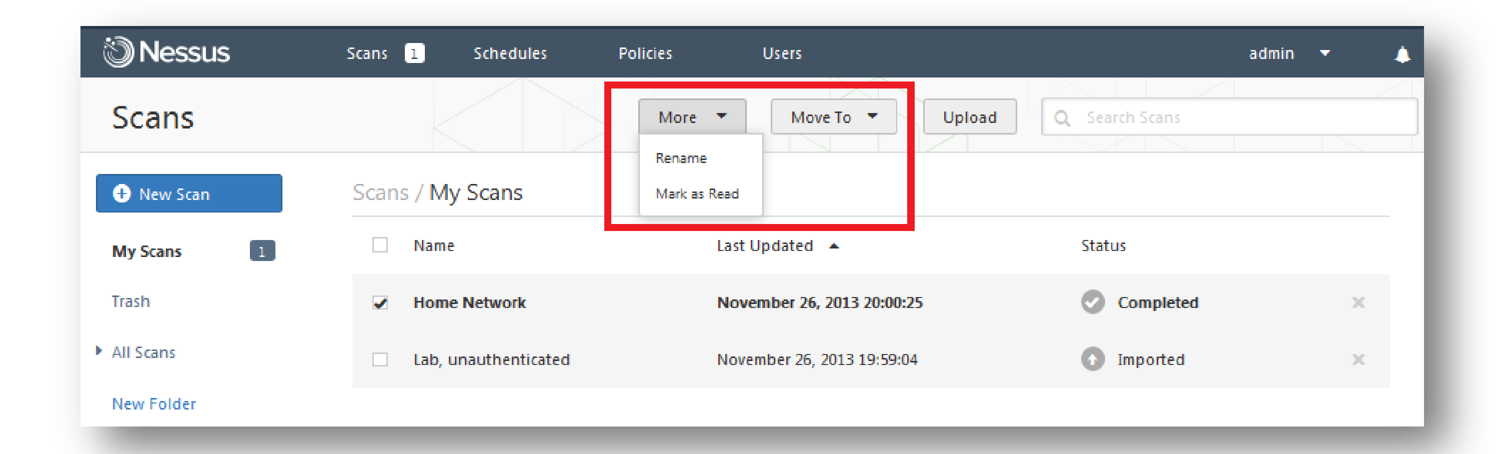


Die Ordner können auch über das Menü „**User Profile**“ > „**Folders**“ („Benutzerprofil“ > „Ordner“) verwaltet werden.

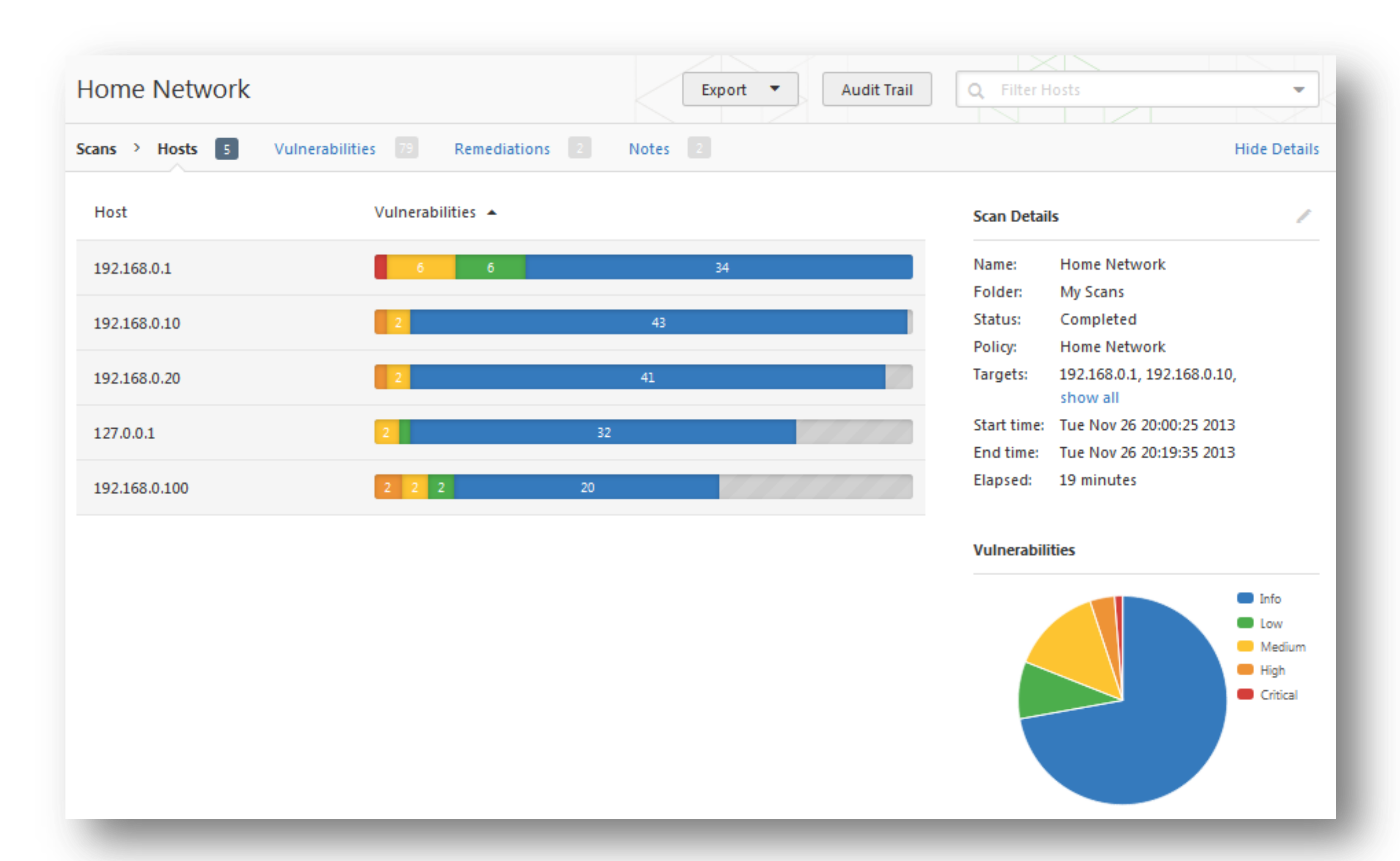


Scans im Ordner „Trash“ werden automatisch nach 30 Tagen gelöscht. Sie können sie jederzeit manuell oder durch Auswahl von „**Empty Trash**“ („Papierkorb leeren“) löschen.

Zum Verschieben von Scanergebnissen in andere Ordner markieren Sie den betreffenden Scan durch Aktivierung des zugehörigen Kontrollkästchens. Nach dem Markieren werden oben weitere Dropdownmenüs angezeigt. Das Menü „More“ („Mehr“) enthält weitere Optionen beispielsweise zum Umbenennen oder zum Markieren als gelesen bzw. nicht gelesen. Das zweite Menü „Move To“ bietet Ihnen die Möglichkeit, den Scan in einen anderen Ordner zu verschieben.



Wählen Sie zum Durchsuchen der Ergebnisse eines Scans einen Bericht aus der Liste aus. Nun können Sie die unterschiedlichen Resultate anzeigen: Navigieren Sie zu Sicherheitslücken oder Hosts und zeigen Sie Ports und spezifische Informationen zu Sicherheitslücken an. In der Standardansicht bzw. auf der Standardregisterkarte ist eine Zusammenfassung nach Hosts dargestellt. Sie zeigt für jeden Hosts eine farblich aufgeschlüsselte Zusammenfassung zu den vorhandenen Sicherheitslücken an:

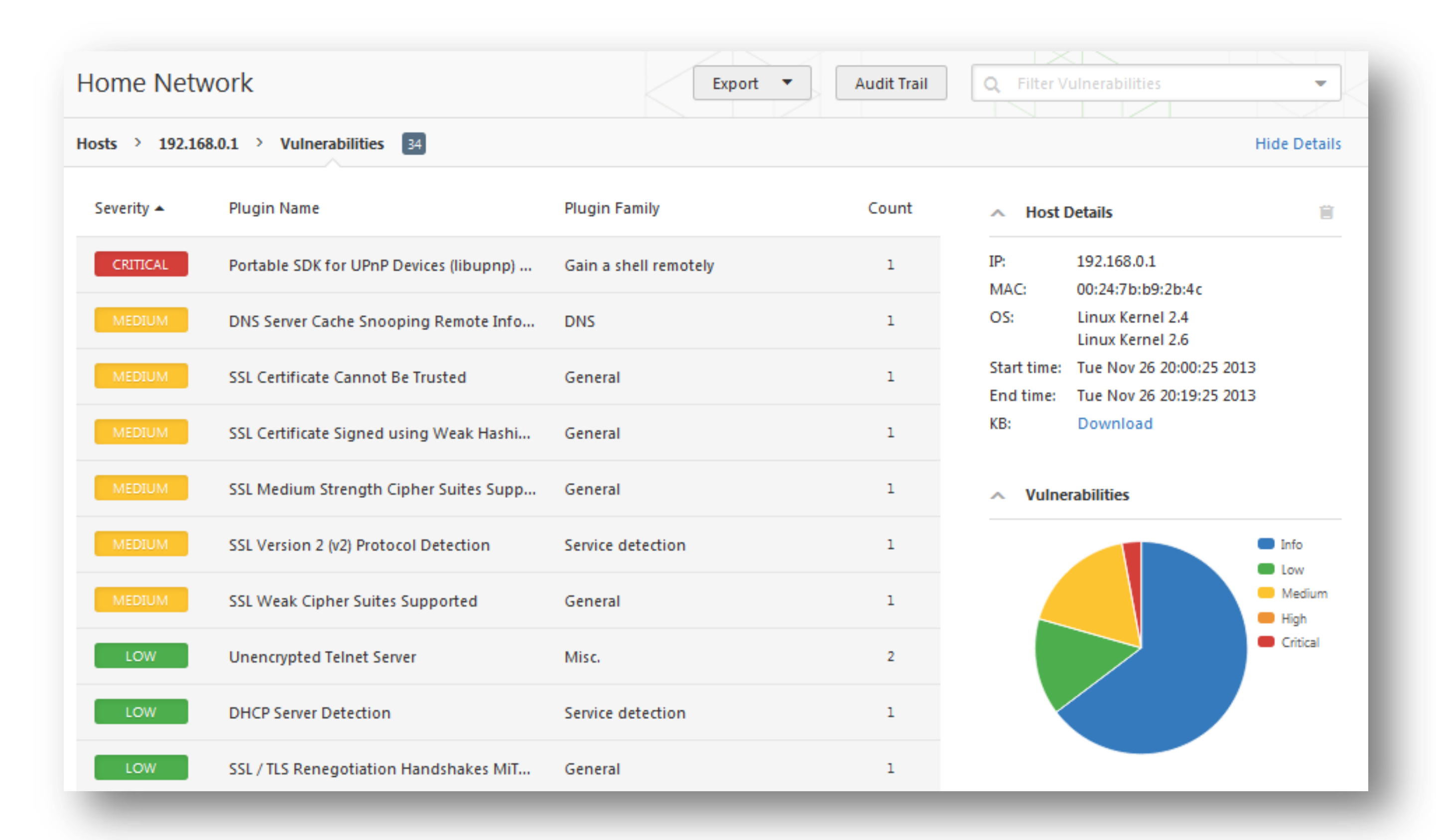


Sind während des Scans Fehler aufgetreten, dann erscheint ein entsprechender Hinweis über den Ergebnissen:

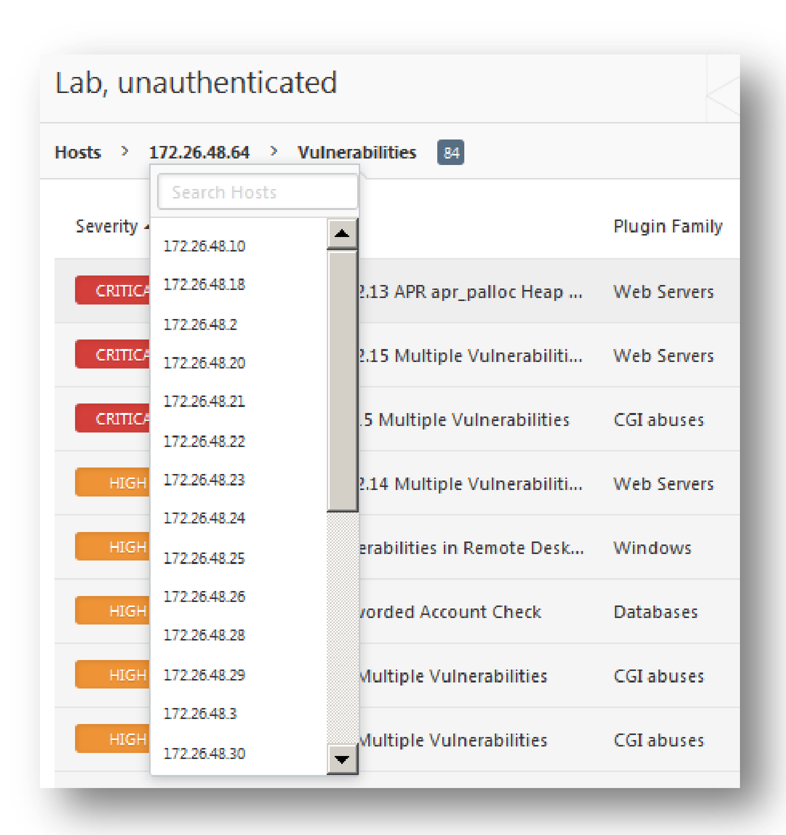
Network interface not supported
The network interface '\Device\{F3957D14-D708-454D-93A7-C7DFF8F076F6}' does not support packet forgery. This prevents Nessus from determining whether some of the target hosts are alive and from performing a full port scan against them. You may partially work around this problem by editing your scan settings to disable 'Ping' (Uncheck General->Ping host) and by providing Nessus with credentials to the remote host to prevent a port scan from taking place, however it would be preferable to scan over a different network interface.

Wenn Sie mehr Zusammenfassungsinformationen anzeigen möchten, klicken Sie oben rechts auf „Hide Details“ („Details ausblenden“), um die Details zu einzelnen Scans auszublenden.

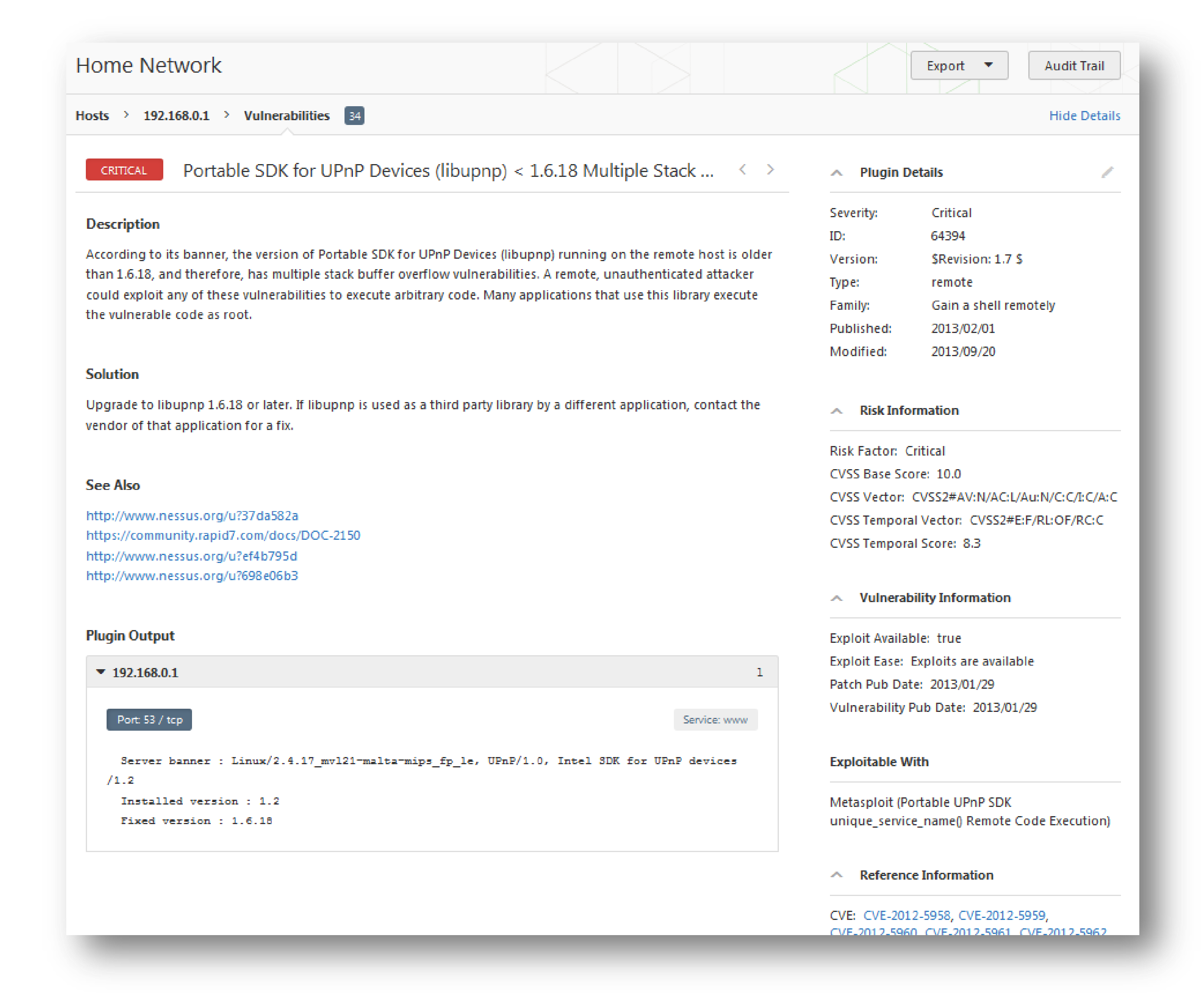
In der Ansicht „Hosts“ enthält jede Zusammenfassung Details zu Sicherheitslücken oder ermittelten Informationen sowie einen Bereich „**Host Details**“ („Hostdetails“), der allgemeine Angaben zum gescannten Host enthält. Wurde „**Allow Post-Scan Report Editing**“ („Nachträgliche Bearbeitung von Berichten gestatten“) in der Scanrichtlinie ausgewählt, dann können Sie einen Host aus den Scanergebnissen löschen, indem Sie das Papierkorbsymbol rechts neben „**Host Details**“ anklicken.



Klicken Sie zum schnellen Wechseln zwischen Hosts oben in der Navigation auf den Host, um ein Pulldownmenü mit den anderen Hosts zu öffnen. Sind sehr viele Hosts vorhanden, dann können Sie über das Suchfeld („Search Hosts“) gezielt nach Hosts suchen:

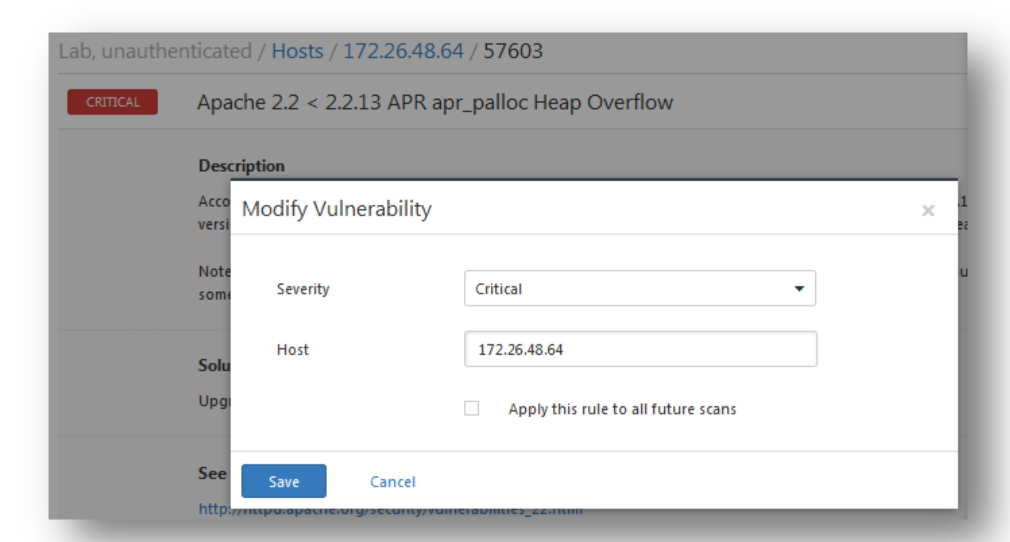


Nach einem Klick auf eine Sicherheitslücke auf den Registerkarten „Hosts“ oder „Vulnerabilities“ werden zugehörige Angaben angezeigt. Hierzu gehören eine Beschreibung, eine Lösung, Referenzen und Ausgaben relevanter Plugins. „**Plugin Details**“ („**Plugin-Details**“) werden auf der rechten Seite angezeigt und enthalten Informationen zum Plugin und der zugehörigen Sicherheitslücke. In diesem Fenster können Sie den Stift rechts neben „**Plugin Details**“ verwenden, um die angezeigte Sicherheitslücke zu ändern:

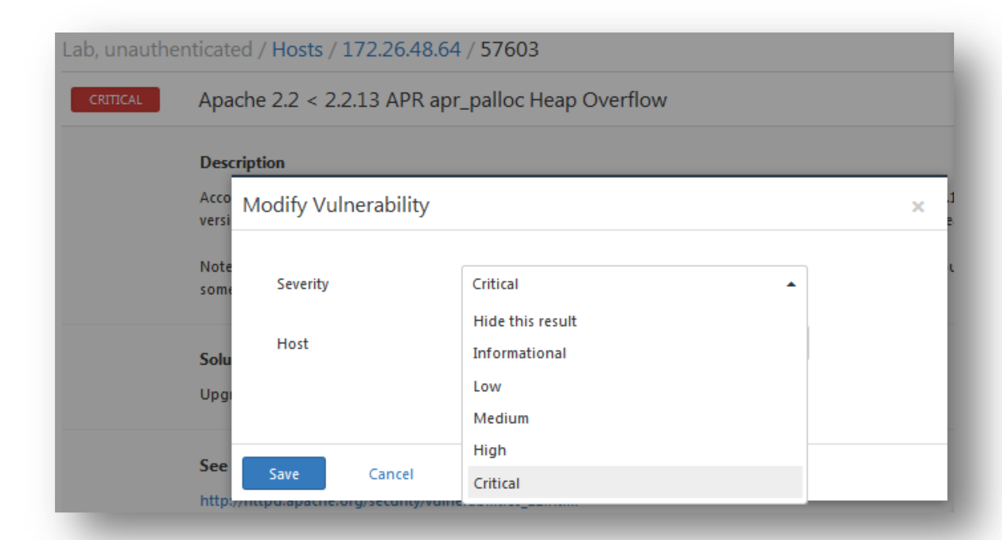


Home Network
Export
Audit Trail
Hosts > 192.168.0.1 > Vulnerabilities 34
Hide Details
CRITICAL
Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack ...
Description
According to its banner, the version of Portable SDK for UPnP Devices (libupnp) running on the remote host is older than 1.6.18, and therefore, has multiple stack buffer overflow vulnerabilities. A remote, unauthenticated attacker could exploit any of these vulnerabilities to execute arbitrary code. Many applications that use this library execute the vulnerable code as root.
Solution
Upgrade to libupnp 1.6.18 or later. If libupnp is used as a third party library by a different application, contact the vendor of that application for a fix.
See Also
http://www.nessus.org/u?37da582a
https://community.rapid7.com/docs/DOC-2150
http://www.nessus.org/u?ef4b795d
http://www.nessus.org/u?698e06b3
Plugin Output
192.168.0.1
1
Port: 53 / tcp
Service: www
Server banner : Linux/2.4.17_mvl21-malta-mips_fp_le, UPnP/1.0, Intel SDK for UPnP devices /1.2
Installed version : 1.2
Fixed version : 1.6.18
Plugin Details
Severity: Critical
ID: 64394
Version: $Revision: 1.7 $
Type: remote
Family: Gain a shell remotely
Published: 2013/02/01
Modified: 2013/09/20
Risk Information
Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C
CVSS Temporal Score: 8.3
Vulnerability Information
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: 2013/01/29
Vulnerability Pub Date: 2013/01/29
Exploitable With
Metasploit (Portable UPnP SDK unique_service_name() Remote Code Execution)
Reference Information
CVE: CVE-2012-5958, CVE-2012-5959,

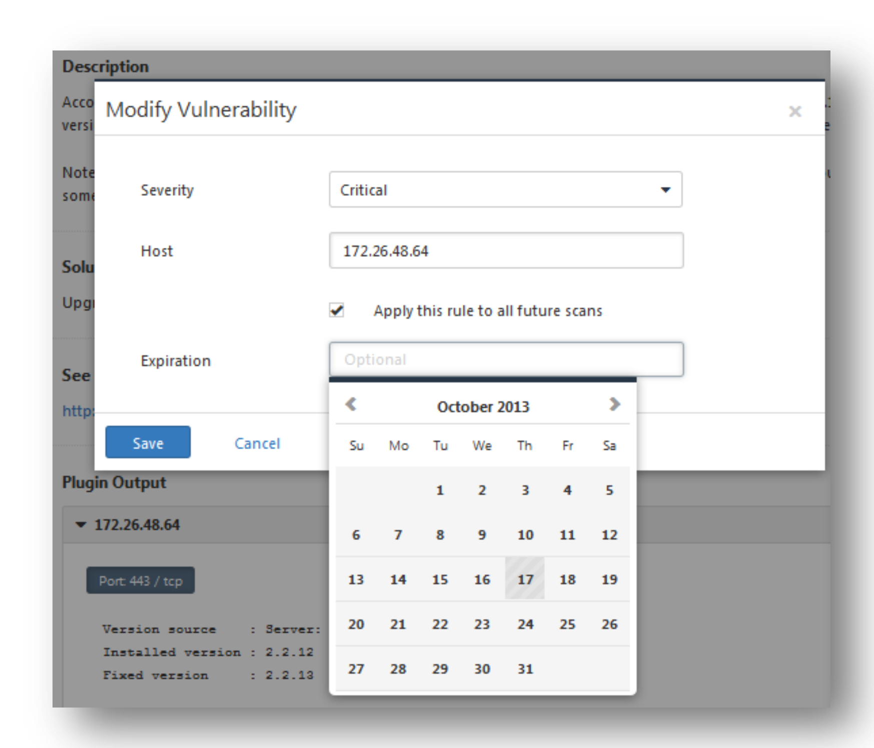
Nach Anklicken des Stiftsymbols wird folgender Dialog angezeigt:



Im Dropdownmenü zum Schweregrad („Severity") können Sie diesen für die betreffende Sicherheitslücke neu angeben oder die Sicherheitslücke im Bericht ausblenden:



Vorgenommene Änderungen werden durch einen Klick auf „**Save**“ gespeichert und für die Sicherheitslücke übernommen. Die Änderung kann zudem für alle weitere Berichte übernommen werden, wenn Sie die betreffende Option „**Apply this rule to all future scans**“ markieren. Dadurch wird ein Dialogfeld geöffnet, in dem Sie bei Bedarf ein Ablaufdatum für die Änderungsregel eingeben können:



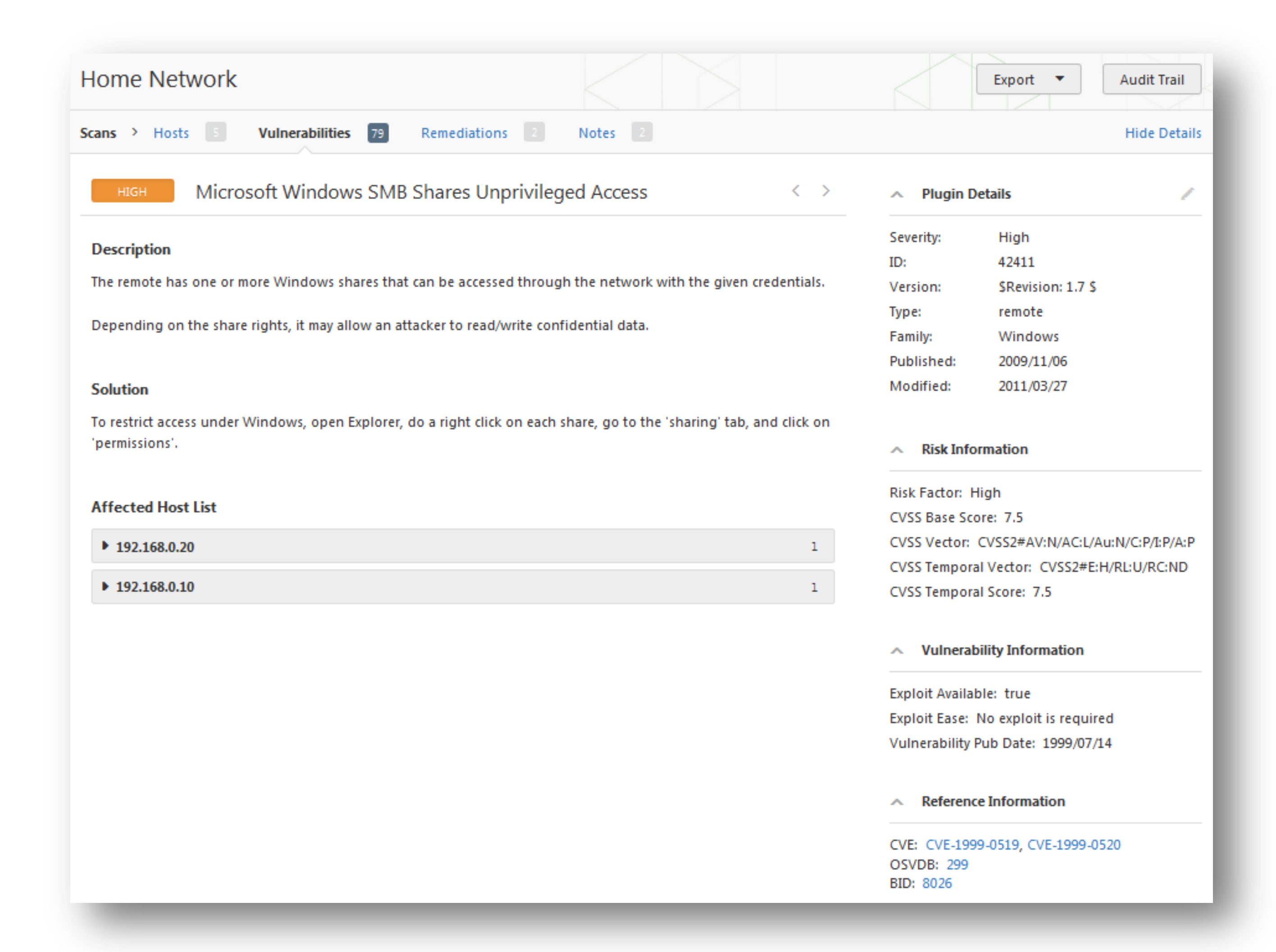
Das Ablaufdatum können Sie im Kalender auswählen. Nach diesem Datum wird die angegebene Änderungsregel nicht mehr auf das Resultat angewandt.

Beachten Sie, dass globale Regeln zur Neubewertung des Risikos oder Schweregrads eines Plugins in Nessus im Bereich „**User Profile**“ > „**Plugin Rules**“ („Benutzerprofil“ > „Plugin-Regeln“) festgelegt werden können.



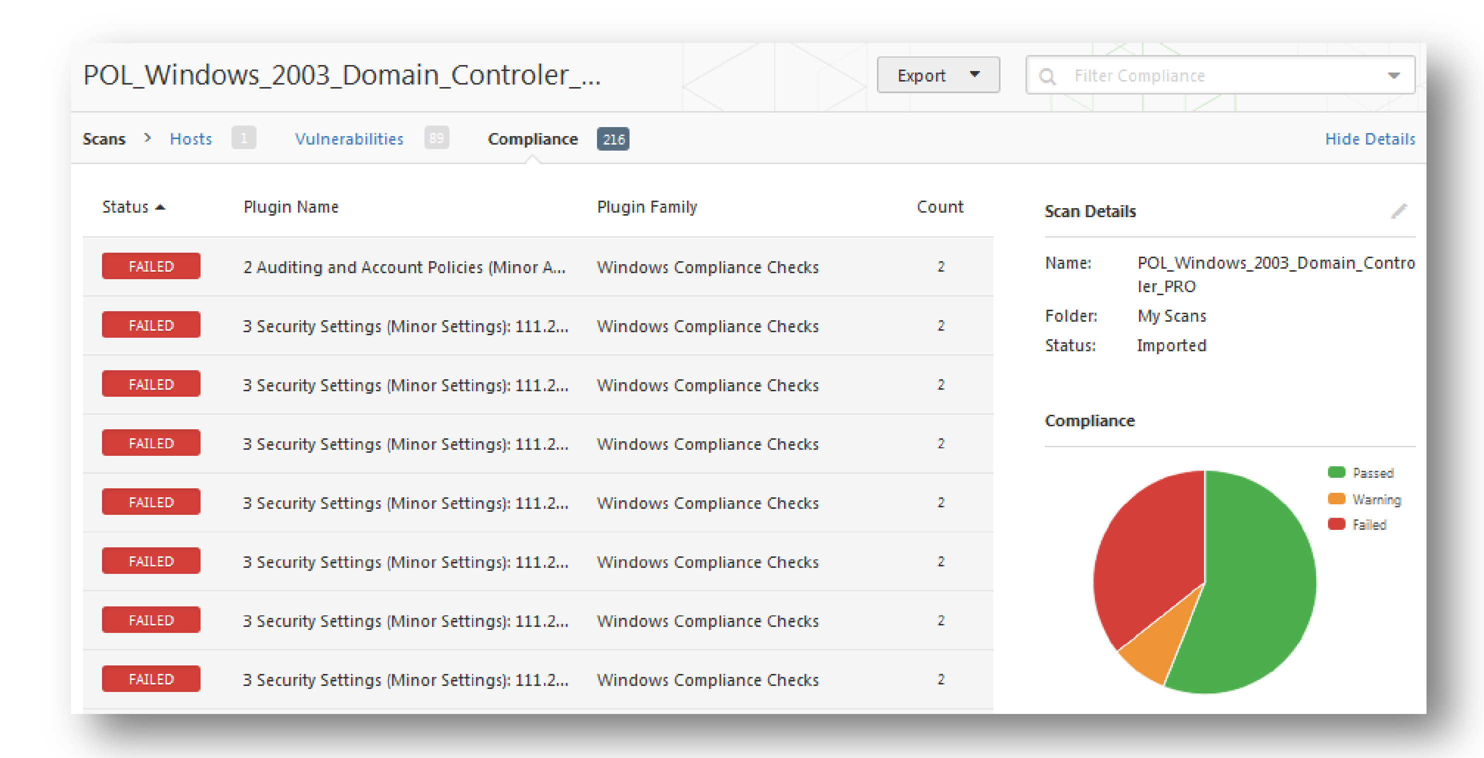
Die Schweregradbewertungen sind von der zugehörigen CVSS-Bewertung abgeleitet. Dabei wird eine Punktzahl von 0 als „Information“, ein Wert von unter 4 als „niedrig“, von unter 7 als „moderat“, von unter 10 als „hoch“ und von 10 oder höher als „kritisch“ gewertet.

Durch Auswählen der Registerkarte „**Vulnerabilities**“ („Sicherheitslücken“) am oberen Bildschirmrand rufen Sie die Sicherheitslückenansicht auf. Die Ergebnisse werden hier nach Sicherheitslücken und nicht nach Hosts sortiert. Die Anzahl der betroffenen Hosts ist auf der rechten Seite angezeigt. Bei Auswahl einer Sicherheitslücke werden dieselben Informationen wie oben, hier jedoch einschließlich einer Liste der betroffenen Hosts unten auf dem Bildschirm angezeigt.

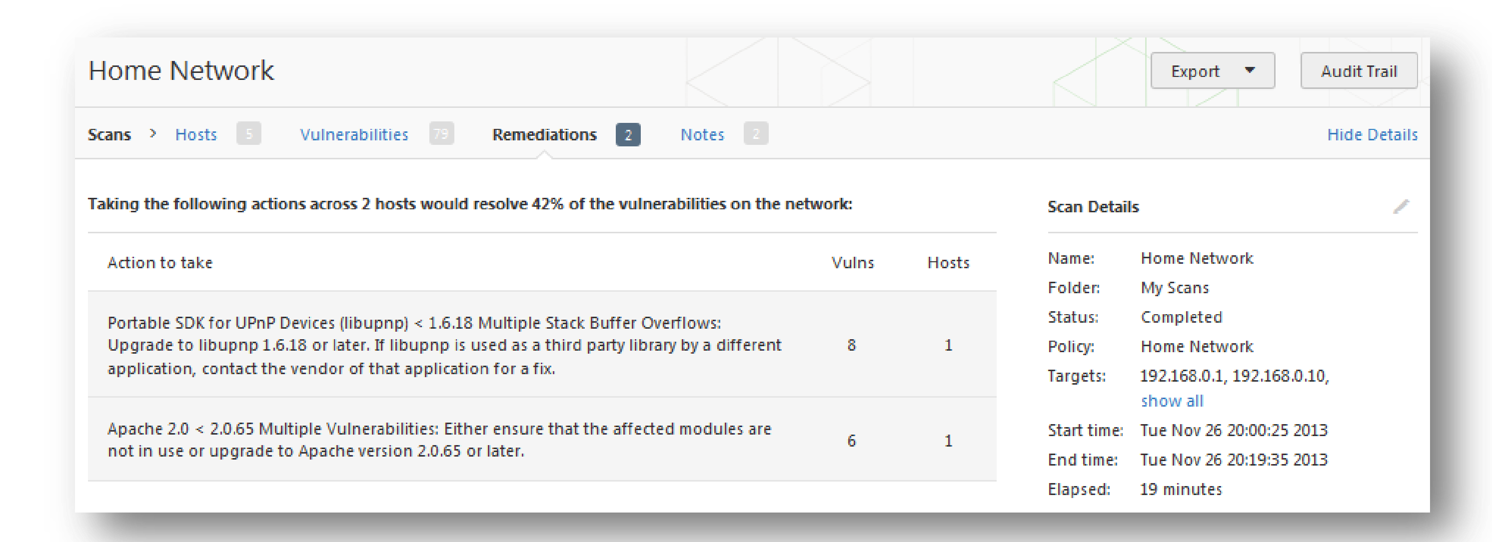


Wenn Sie auf einen betroffenen Host klicken, wird die hostbasierte Sicherheitslückenansicht geladen.

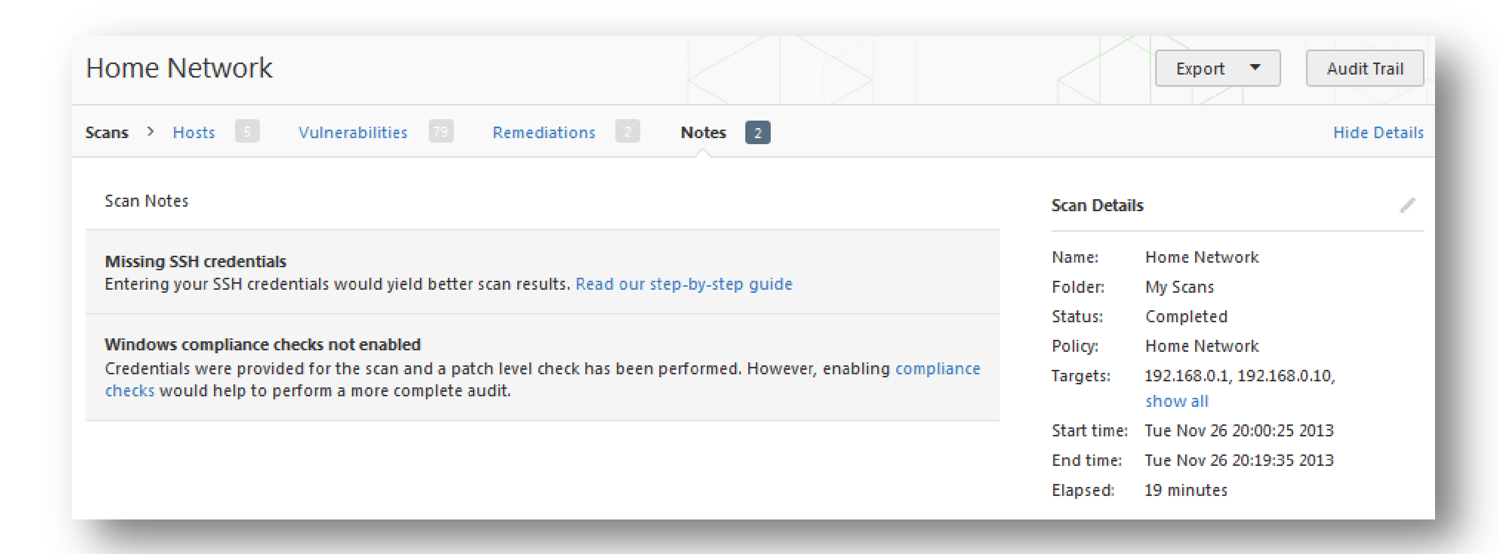
Wird ein Scan gestartet, der eine Compliancerichtlinie verwendet, finden Sie die Ergebnisse auf der separaten Registerkarte „**Compliance**“ oben auf dem Bildschirm:



Neben „**Hosts**“ und „**Vulnerabilities**“ bietet Nessus zwei weitere Registerkarten. Die erste heißt „**Remediations**“ („Korrekturen“) und enthält zusammenfassende Angaben zur Behebung schwerwiegender erkannter Probleme. Die enthaltenen Hinweise sollen Ihnen die effektivsten Abhilfemaßnahmen nennen, mit denen sich die Anzahl der Sicherheitslücken erheblich reduzieren lässt:



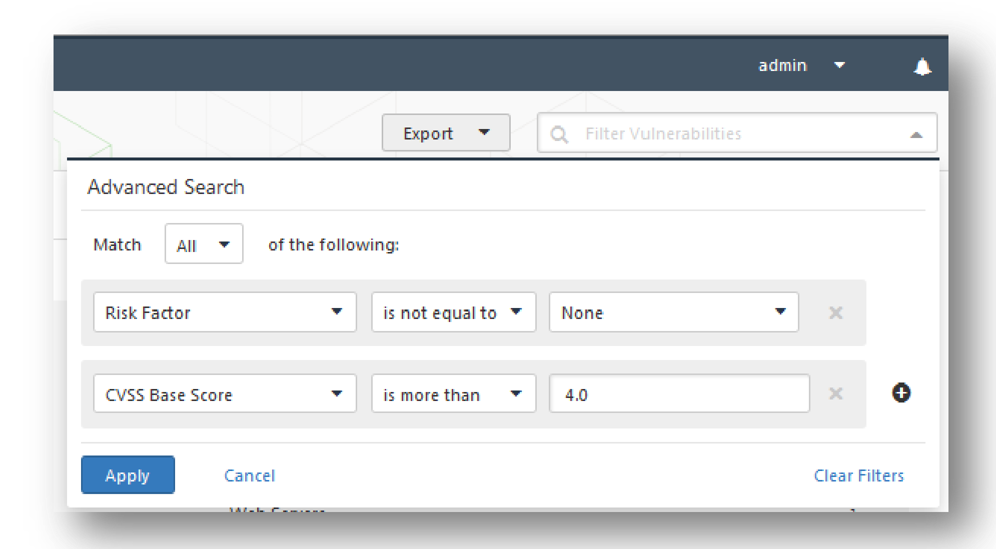
Die zweite Registerkarte heißt „Notes“ („Hinweise“). Sie vermittelt Ratschläge, wie Sie Ihre Scanergebnisse verbessern können:



Berichtsfilter

Nessus bietet ein flexibles Filtersystem, mit dem die Anzeige bestimmter Berichtsresultate vereinfacht wird. Mithilfe von Filtern lassen sich Ergebnisse basierend auf jedem beliebigen Aspekt der gefundenen Sicherheitslücken anzeigen. Werden mehrere Filter verwendet, dann lassen sich detaillierte und angepasste Berichtsansichten erstellen.

Der erste Filtertyp ist eine einfache Textzeichenfolge, die in das Feld „**Filter Vulnerabilities**“ („Sicherheitslücken filtern“) oben rechts eingegeben wird. Bereits beim Eingeben beginnt Nessus mit der Filterung der Ergebnisse auf der Basis Ihrer Eingabe und der Übereinstimmungen in den Resultaten. Der zweite Filtertyp ist umfassender und ermöglicht die Eingabe zusätzlicher Einzelheiten. Zur Einrichtung dieses Filters klicken Sie zunächst auf den Abwärtspfeil rechts neben „**Filter Vulnerabilities**“. Filter können auf jeder Berichtsregisterkarte erstellt werden. Mehrere Filter können durch logische Bedingungen verknüpft werden, was eine komplexe Filterung gestattet. Ein Filter wird durch Auswahl des Plugin-Attributs, eines Filterarguments und eines zu filternden Werts erstellt. Geben Sie bei Auswahl mehrerer Filter das Schlüsselwort „Any“ („beliebig“) oder „All“ („alle“) entsprechend an. Bei Auswahl von „All“ werden Ergebnisse angezeigt, die die Kriterien **aller** Filter erfüllen:



Nach Einrichtung eines Filters kann er durch Klicken auf ✖ rechts davon entfernt werden. Durch Auswahl von „**Clear Filters**“ („Alle Filter löschen“) können alle Filter entfernt werden. Die Berichtsfilter unterstützen eine Vielzahl von Kriterien zur fein abgestuften Steuerung der Ergebnisse:

Option	Beschreibung
Plugin ID (Plugin-ID)	Filtert Ergebnisse, wenn die Plugin-ID einer bestimmten Zeichenfolge (z. B. 42111) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Plugin Description (Plugin-Beschreibung)	Filtert Ergebnisse, wenn die Plugin-Beschreibung eine bestimmte Zeichenfolge (z. B. „remote“) enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Plugin Name (Plugin-Name)	Filtert Ergebnisse, wenn der Plugin-Name einer bestimmten Zeichenfolge (z. B. „windows“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Plugin Family (Plugin-Familie)	Filtert Ergebnisse, wenn der Plugin-Name einer der angegebenen Nessus-Plugin-Familien entspricht („*is equal to*“) bzw. nicht entspricht („*is not equal to*“). Die möglichen Entsprechungen werden über ein Dropdownmenü bereitgestellt.
Plugin Output (Plugin-Ausgabe)	Filtert Ergebnisse, wenn die Plugin-Beschreibung einer bestimmten Zeichenfolge (z. B. „PHP“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Plugin Type (Plugin-Typ)	Filtert Ergebnisse, wenn der Plugin-Typ einem der folgenden beiden Plugin-Typen entspricht („*is equal to*“) bzw. nicht entspricht („*is not equal to*“): „local“ („lokal“), „remote“.
Solution (Lösung)	Filtert Ergebnisse, wenn die Plugin-Lösung eine bestimmte Zeichenfolge (z. B. „upgrade“) enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Synopsis (Zusammenfassung)	Filtert Ergebnisse, wenn die Plugin-Zusammenfassung eine bestimmte Zeichenfolge (z. B. „PHP“) enthält („*contains*“) bzw. nicht enthält („*does not contain*“).

Hostname	Filtert Ergebnisse, wenn der Host einer bestimmten Zeichenfolge (z. B. „192.168“ oder „lab“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Port	Filtert Ergebnisse basierend darauf, ob ein Port einer bestimmten Zeichenfolge (z. B. „80“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Protocol (Protokoll)	Filtert Ergebnisse, wenn ein Protokoll einer bestimmten Zeichenfolge (z. B. „http“) entspricht („*is equal to*“) bzw. nicht entspricht („*is not equal to*“).
CPE	Filtert Ergebnisse basierend darauf, ob die Common Platform Enumeration (CPE) einer bestimmten Zeichenfolge (z. B. „solaris“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
CVSS Base Score (CVSS-Basisbewertung)	Filtert Ergebnisse basierend darauf, ob die CVSS-Basisbewertung kleiner („*is less than*“) oder größer („*is more than*“) als eine bestimmte Zeichenfolge (z. B. „5“) ist, der Zeichenfolge entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“). Mithilfe dieses Filters kann nach Risikostufe ausgewählt werden. Die Schweregradbewertungen sind von der zugehörigen CVSS-Bewertung abgeleitet. Dabei wird eine Punktzahl von 0 als „Information“, ein Wert von unter 4 als „niedrig“, von unter 7 als „moderat“, von unter 10 als „hoch“ und von 10 oder höher als „kritisch“ gewertet.
CVSS Temporal Score (CVSS-Temporärbewertung)	Filtert Ergebnisse basierend darauf, ob die CVSS-Temporärbewertung kleiner („*is less than*“) oder größer („*is more than*“) als eine bestimmte Zeichenfolge (z. B. „3.3“) ist, der Zeichenfolge entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
CVSS Temporal Vector (CVSS-Temporärvektor)	Filtert Ergebnisse basierend darauf, ob der CVSS-Temporärvektor einer bestimmten Zeichenfolge (z. B. „E:F“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
CVSS Vector (CVSS-Vektor)	Filtert Ergebnisse basierend darauf, ob der CVSS-Vektor einer bestimmten Zeichenfolge (z. B. „AV:N“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Vulnerability Publication Date (Veröffentlichungsdatum der Sicherheitslücke)	Filtert Ergebnisse basierend darauf, ob das Veröffentlichungsdatum einer Sicherheitslücke zeitlich früher („*earlier than*“) oder später („*later than*“) als eine Zeichenfolge (z. B. „01/01/2012“) liegt, dem Wert der Zeichenfolge entspricht („*on*“) oder nicht entspricht („*not on*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“). Hinweis: Wenn Sie auf die Schaltfläche neben dem Datum klicken, wird ein Kalender angezeigt, in dem Sie das Datum auswählen können.
Patch Publication Date (Veröffentlichungsdatum des Patchs)	Filtert Ergebnisse basierend darauf, ob das Veröffentlichungsdatum des Patchs zu einer Sicherheitslücke kleiner („*is less than*“) oder größer („*is more than*“) als eine bestimmte Zeichenfolge (z. B. „12/01/2011“) ist, der Zeichenfolge entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).

Plugin Publication Date (Veröffentlichungsdatum des Plugins)	Filtert Ergebnisse basierend darauf, ob das Veröffentlichungsdatum eines Nessus-Plugins kleiner („*is less than*“) oder größer („*is more than*“) als eine bestimmte Zeichenfolge (z. B. „06/03/2011“) ist, der Zeichenfolge entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Plugin Modification Date (Änderungsdatum des Plugins)	Filtert Ergebnisse basierend darauf, ob das Änderungsdatum eines Nessus-Plugins kleiner („*is less than*“) oder größer („*is more than*“) als eine bestimmte Zeichenfolge (z. B. „02/14/2010“) ist, der Zeichenfolge entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
CVE	Filtert Ergebnisse basierend darauf, ob ein CVE-Verweis einer bestimmten Zeichenfolge (z. B. „2011-0123“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Bugtraq ID (BugTraq-ID)	Filtert Ergebnisse basierend darauf, ob eine Bugtraq-ID einer bestimmten Zeichenfolge (z. B. „51300“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
CERT Advisory ID (CERT-Advisory-ID)	Filtert Ergebnisse basierend darauf, ob eine CERT Advisory ID (heißt mittlerweile „Technical Cyber Security Alert“) einer bestimmten Zeichenfolge (z. B. „TA12-010A“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
OSVDB ID	Filtert Ergebnisse basierend darauf, ob eine Open Source Vulnerability Database (OSVDB)-ID einer bestimmten Zeichenfolge (z. B. „78300“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Secunia ID	Filtert Ergebnisse basierend darauf, ob eine Secunia ID einer bestimmten Zeichenfolge (z. B. „47650“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Exploit Database ID	Filtert Ergebnisse basierend darauf, ob eine Exploit Database ID (EBD-ID) einer bestimmten Zeichenfolge (z. B. „18380“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Metasploit Name (Metasploit-Name)	Filtert Ergebnisse basierend darauf, ob ein Metasploit-Name einer bestimmten Zeichenfolge (z. B. „xslt_password_reset“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Exploit Hub	Filtert Ergebnisse basierend darauf, ob ein ExploitHub-Exploit wahr („*true*“) oder falsch („*false*“) ist.
IAVA	Filtert Ergebnisse basierend darauf, ob eine IAVA-Referenz einer bestimmten Zeichenfolge (z. B. „2012-A-0008“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
IAVB	Filtert Ergebnisse basierend darauf, ob eine IAVB-Referenz einer bestimmten Zeichenfolge (z. B. „2012-A-0008“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
IAVT	Filtert Ergebnisse basierend darauf, ob eine IAVT-Referenz einer bestimmten Zeichenfolge (z. B. „2012-A-0008“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).

See Also (Siehe auch)	Filtert Ergebnisse basierend darauf, ob ein „See also“-Verweis (Querverweis) eines Nessus-Plugins einer bestimmten Zeichenfolge (z. B. „seclists.org“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
Exploits Available (Exploits verfügbar)	Filtert Ergebnisse basierend darauf, ob für die betreffende Sicherheitslücke ein Exploit existiert.
Exploitability Ease	Filtert Ergebnisse basierend darauf, ob die „Exploitability Ease“ (also die Frage, wie einfach die Sicherheitslücke genutzt werden kann) einem der folgenden Werte entspricht („*is equal to*“) bzw. nicht entspricht („*is not equal to*“): „*Exploits are available*“ („Exploits vorhanden“), „*No exploit is required*“ („Keine Exploits benötigt“) oder „*No known exploits are available*“ („Keine bekannten Exploits vorhanden“).
Metasploit Exploit Framework	Filtert Ergebnisse basierend darauf, ob eine Sicherheitslücke im Metasploit Exploit Framework aufgeführt ist („true“) oder nicht („false“).
CANVAS Exploit Framework	Filtert Ergebnisse basierend darauf, ob eine Sicherheitslücke im CANVAS Exploit Framework aufgeführt ist („true“) oder nicht („false“).
CANVAS-Paket	Filtert Ergebnisse basierend darauf, für welches CANVAS Exploit Framework-Paket ein Exploit vorhanden ist. Mögliche Werte sind „CANVAS“, „D2ExploitPack“ und „White_Phosphorus“.
CORE Exploit Framework	Filtert Ergebnisse basierend darauf, ob eine Sicherheitslücke im CORE Exploit Framework aufgeführt ist („true“) oder nicht („false“).
Elliot Exploit Framework	Filtert Ergebnisse basierend darauf, ob eine Sicherheitslücke im Elliot Exploit Framework einem der Werte „true“ („wahr“) oder „false“ („falsch“) entspricht („*is equal to*“) bzw. nicht entspricht („*is not equal to*“).
Elliot Exploit Name	Filtert Ergebnisse basierend darauf, ob der Elliot Exploit einer bestimmten Zeichenfolge (z. B. „Typo3 FD“) entspricht („*is equal to*“) oder nicht entspricht („*is not equal to*“) oder sie enthält („*contains*“) bzw. nicht enthält („*does not contain*“).
ExploitHub	Filtert Ergebnisse basierend darauf, ob eine Sicherheitslücke auf der ExploitHub-Website einem der Werte „true“ („wahr“) oder „false“ („falsch“) entspricht („*is equal to*“) bzw. nicht entspricht („*is not equal to*“).

Bei der Verwendung eines Filters kann der String bzw. der Zahlenwert auch kommagetrennt sein, um nach mehreren Strings zu filtern. Um beispielsweise nur Ergebnisse anzuzeigen, die sich auf Webserver beziehen, könnten Sie einen Filter „Ports“ erstellen, als Filterbedingung „is equal to“ und als Eingabewert „80,443,8000,8080“ festlegen. Auf diese Weise werden Ihnen nur Ergebnisse zu diesen vier Ports angezeigt.



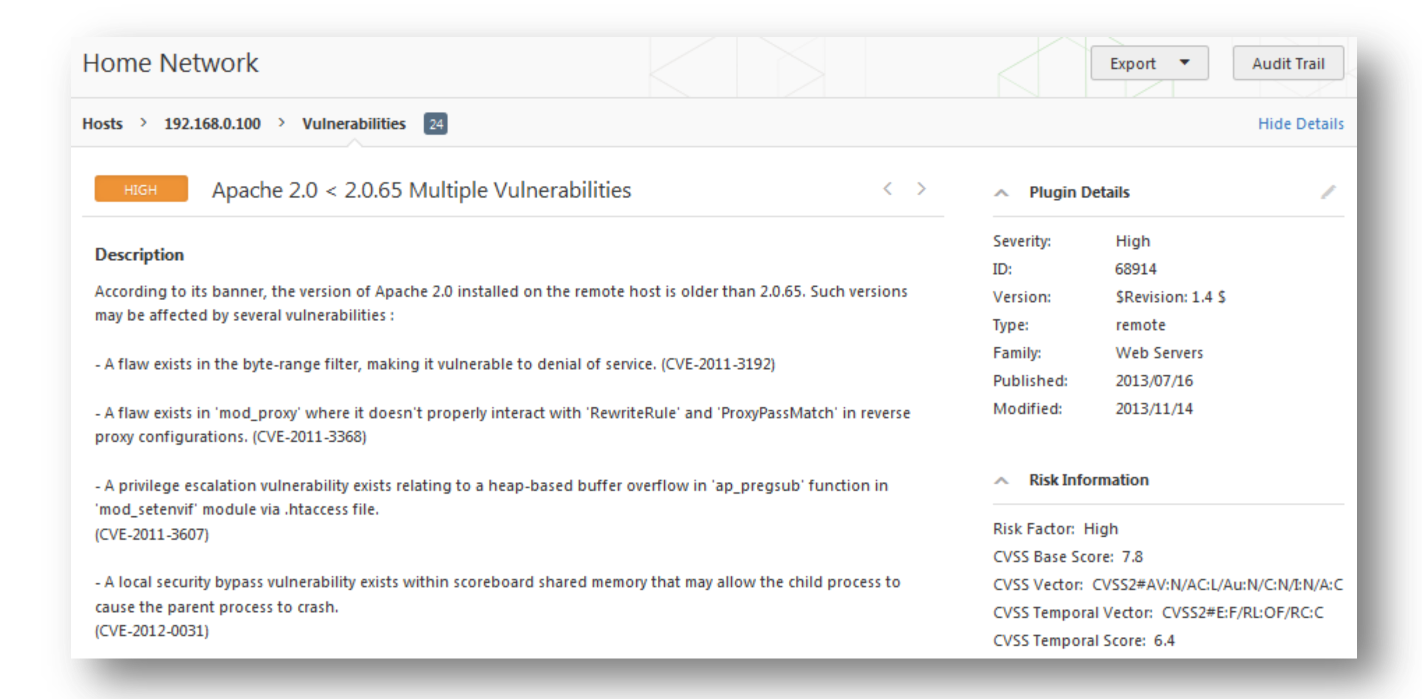
Bei Filterkriterien wird die Groß-/Kleinschreibung nicht unterschieden.

Wenn eine Filteroption nicht verfügbar ist, bedeutet dies, dass der Bericht keine den Kriterien entsprechenden Inhalte hat. Ist beispielsweise „Microsoft Bulletin“ nicht in der Filter-Dropdownliste vorhanden, dann wurden keine Sicherheitslücken gefunden, die auf ein Microsoft-Bulletin verweisen.

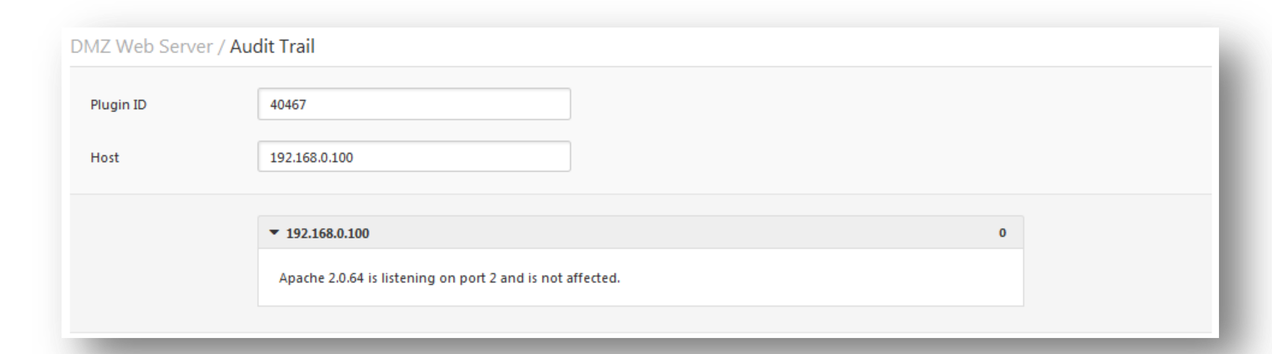
Sobald ein Filter erstellt ist, werden die Scanergebnisse nach Auswahl von „**Apply**“ („Anwenden“) entsprechend den neuen Filterkriterien aktualisiert. Der Abwärtspfeil im Feld „**Filter Vulnerabilities**“ („Sicherheitslücken filtern“) zeigt nun numerisch an, wie viele Filter derzeit angewendet werden.

Wenn die Ergebnisse so gefiltert wurden, dass die von Ihnen gewünschten Daten angezeigt werden, können Sie auf „**Export Results**“ („Ergebnisse exportieren“) klicken, um nur die gefilterten Ergebnisse zu exportieren. Entfernen Sie für Berichte mit allen Ergebnissen alle Filter und verwenden Sie dann die Exportfunktion.

Die Nessus-Scanergebnisse bieten Ihnen einen schnellen Überblick über Plugins, von denen Probleme auf dem Host gefunden wurden. Manchmal werden Sie allerdings wissen wollen, warum ein Plugin **keine** Ergebnisse zurückgegeben hat. Hierfür ist die Funktion „**Audit Trail**“ gedacht. Klicken Sie zunächst auf das Symbol „Audit Trail“ oben rechts auf dem Bildschirm:



Dadurch wird der Dialog „Audit Trail“ aufgerufen. Geben Sie nun die ID des Plugins ein, über das Sie mehr erfahren möchten. Klicken Sie auf „**Submit**“ („Senden“). Nun werden ein oder mehrere Hosts angezeigt, die Ihrer Abfrage entsprechen. Optional können Sie eine Host-IP-Adresse bei der ersten Abfrage angeben, um die Ergebnisse auf das gewünschte Ziel zu beschränken. Wenn der oder die gefundenen Hosts angezeigt werden, klicken Sie auf die gewünschte Information, um zu erfahren, warum ein Plugin kein Ergebnis gefunden hat:



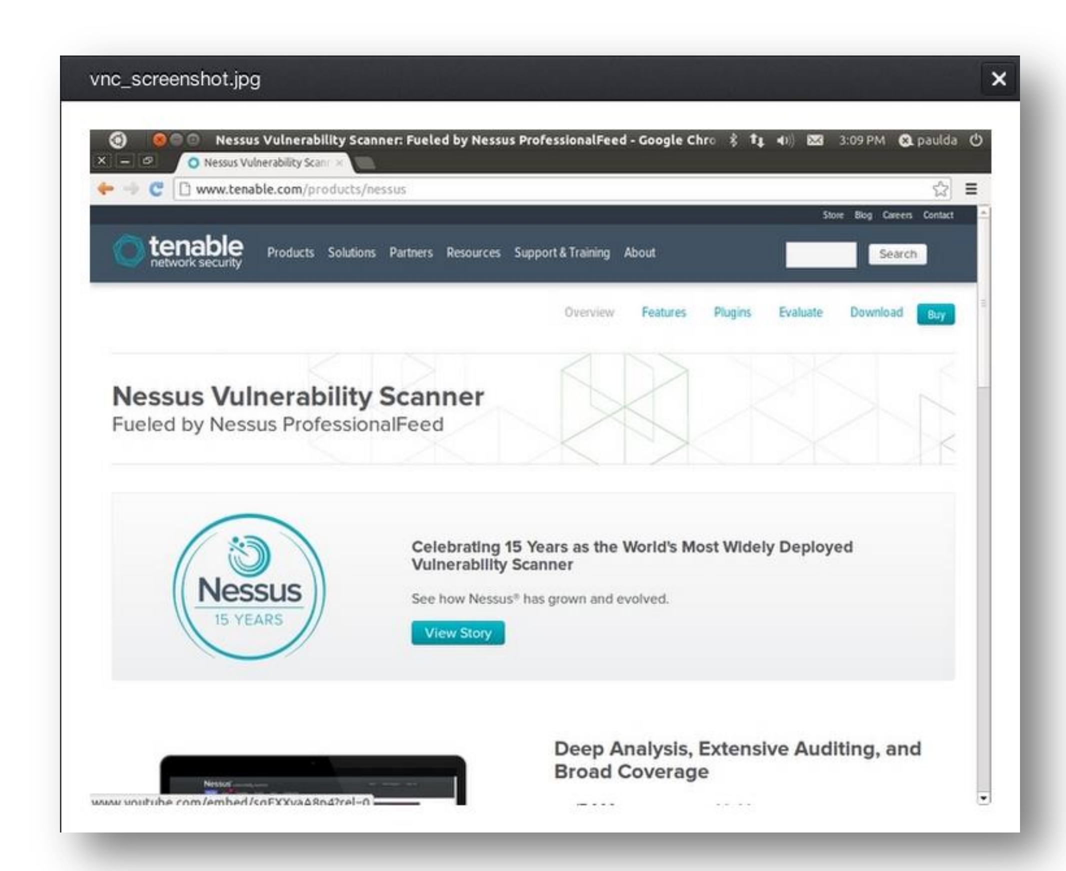


Da ein Audit-Trail sehr ressourcenintensiv ist, stehen unter bestimmten Umständen nur eingeschränkte Audit-Trails zur Verfügung. Wird nur ein Host gescannt, dann erfolgt der Audit-Trail vollständig. Bei zwei bis 512 gescannten Hosts sind für einen vollständigen Audit-Trail mindestens zwei CPUs und 2 GB Arbeitsspeicher erforderlich. Bei mehr als 512 Hosts wird immer nur ein eingeschränkter Audit-Trail ausgeführt.

Der Audit-Trail ist nur für Scans verfügbar, die vom betreffenden Host stammen. Bei importierten Scans funktioniert er nicht.

Berichtscreenshots

Nessus 5.2 kann während des Sicherheitslückenscans Screenshots (Bildschirmabbildungen) erstellen, die in den Bericht aufgenommen werden. Wenn Nessus beispielsweise erkennt, dass ein VNC ohne Kennwort zur Zugriffsbeschränkung ausgeführt wird, wird ein Screenshot der Sitzung aufgenommen und dem Bericht hinzugefügt. Im folgenden Beispiel wurde ein VNC erkannt, als der Benutzer die Tenable-Website aufrief:

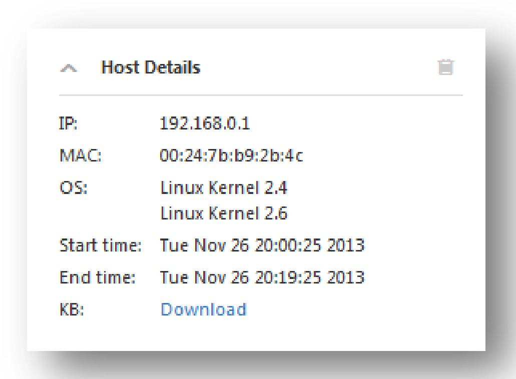


Die Funktion muss im Abschnitt „**Preferences**" („Voreinstellungen") der Scanrichtlinie unter „**Remote web server screenshot**" („Screenshot des Remotewebservers") aktiviert werden. Weitere Informationen finden Sie im Abschnitt „Scanvoreinstellungen im Detail" dieses Dokuments.

Scan Knowledge Base (Scan Knowledge-Base)

Bei jedem Scan wird eine Wissensdatenbank (Knowledge Base, KB) gespeichert. Es handelt sich hierbei um eine ASCII-Textdatei mit Protokollangaben zum durchgeführten Scan und den gefundenen Ergebnissen. Eine KB ist häufig nützlich, wenn Sie Unterstützung von Tenable benötigen: Mit ihrer Hilfe kann der Supportmitarbeiter nachvollziehen, was genau Nessus tat und welche Daten gefunden wurden.

Wählen Sie zum Laden einer KB einen Bericht und dann den gewünschten Host aus. Klicken Sie rechts neben dem Hostnamen oder der IP-Adresse auf den Link „**Host Details**“ („Hostdetails“). Nun wird unter anderem die Option „**KB**“ mit einem Link „**Download**“ angezeigt:



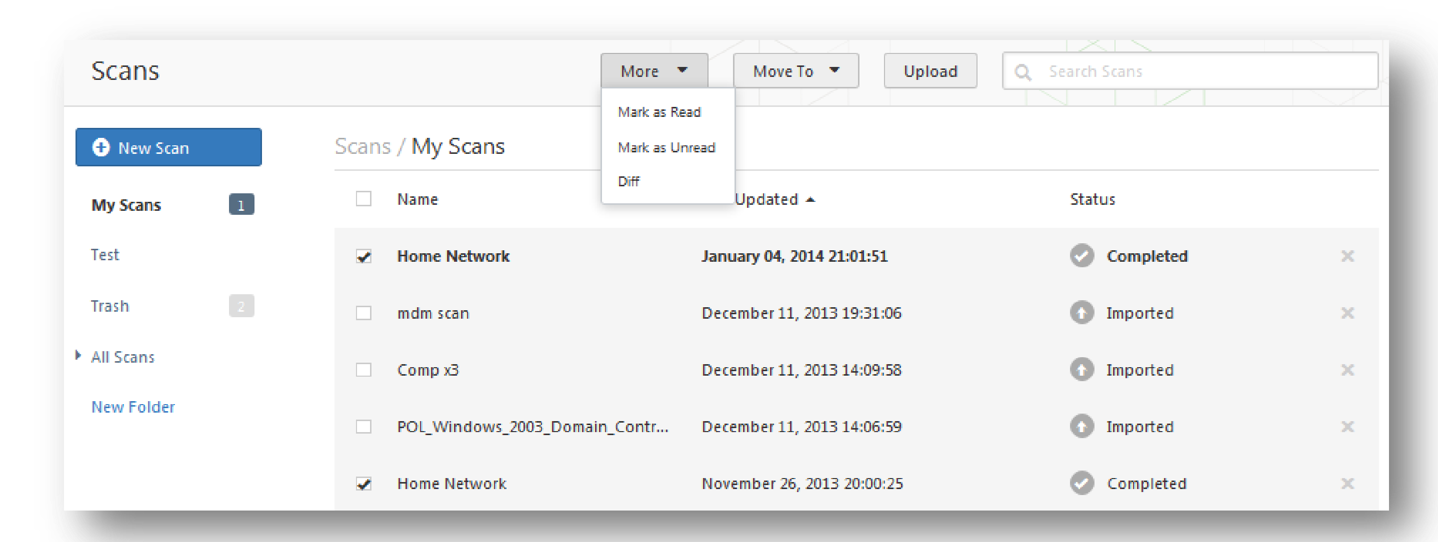


Nur für auf dem Host ausgeführte Scans ist eine KB vorhanden. In importierten Scans sind keine KB-Informationen gespeichert.

Vergleichsfunktion („Diff“)

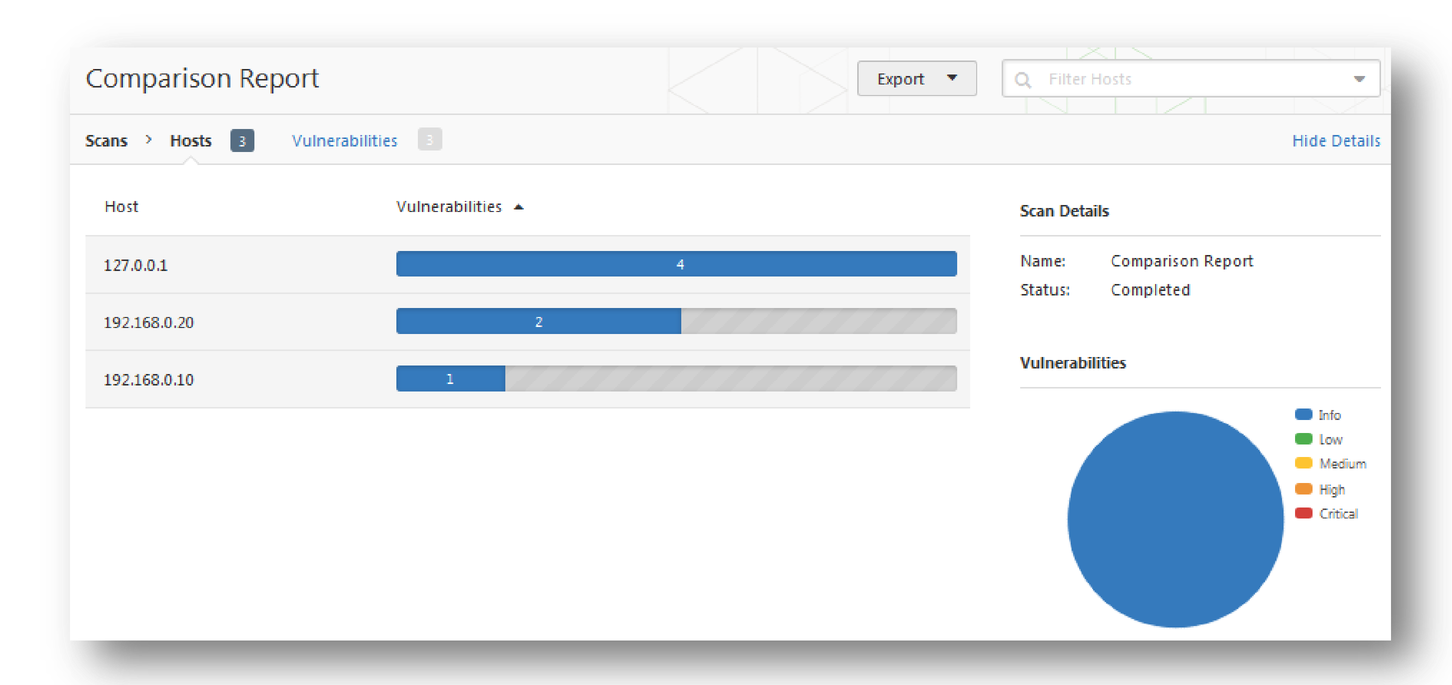
In Nessus können Sie zwei Scanberichte miteinander vergleichen, um Unterschiede anzuzeigen. Durch die Möglichkeit, Unterschiede zwischen Scans anzuzeigen, lässt sich feststellen, wie sich ein gegebenes System oder Netzwerk im Laufe der Zeit verändert hat. Dies erleichtert Complianceanalysen, denn Sie können so erkennen, welche Sicherheitslücken geschlossen wurden, ob Systeme bei Feststellung neuer Sicherheitslücken entsprechend gepatcht wurden oder dass zwei Scans möglicherweise nicht die gleichen Hosts verarbeiten.

Starten Sie den Vergleich von Berichten, indem Sie zwei Scans aus der Liste „**Scans**“ wählen, dann auf „**More**“ („Mehr“) klicken und „**Diff**“ („Unterschiede“) aus dem Dropdownmenü wählen:



Nessus vergleicht den ersten ausgewählten Bericht mit dem zweiten und generiert eine Liste mit Ergebnissen, die sich seit dem ersten Bericht geändert haben. Die Vergleichsfunktion zeigt nicht die Unterschiede zwischen zwei beliebigen Berichten, sondern stellt die Änderungen dar, die seit dem ersten Bericht (der Baseline) stattgefunden haben. An diesen

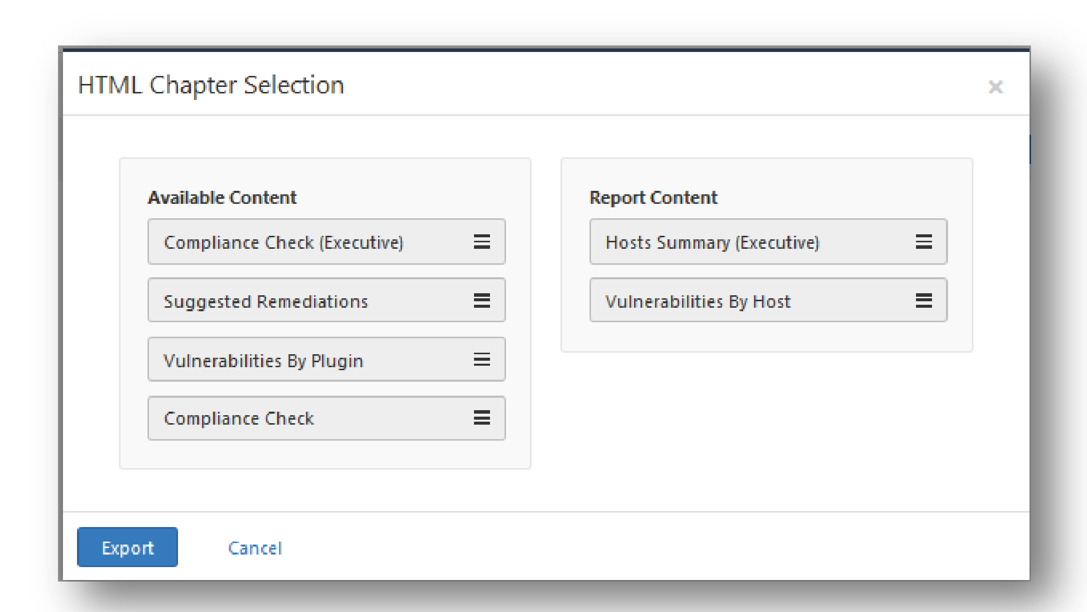
Ergebnissen lässt sich also ablesen, welche Sicherheitslücken zwischen den beiden Scans gefunden bzw. behoben wurden. In dem oben genannten Beispiel ist „DMZ Web Server“ ein nicht authentifizierter Scan auf einem einzelnen Webserver in einer DMZ, der mehrmals ausgeführt wurde Die Ergebnisse zeigen die Unterschiede an, wobei die Sicherheitslücken hervorgehoben sind, die im Scan vom 7. Oktober nicht gefunden wurden:



Upload und Export

Scanergebnisse können aus einem Nessus-Scanner exportiert und in einen anderen importiert werden. Die Funktionen „**Upload**“ („Hochladen“) und „**Export**“ erleichtern Scanmanagement, Berichtsvergleich, Sicherung von Berichten und die Kommunikation zwischen Gruppen und Organisationen innerhalb eines Unternehmens.

Beginnen Sie den Export eines Scans durch Auswahl des Berichts im Bildschirm „**Scans**“. Klicken Sie dann auf das Dropdownmenü „**Export**“ oben auf dem Bildschirm und legen Sie das gewünschte Format fest. Daraufhin wird ein Fenster angezeigt, in das Sie die einzuschließenden (in „Kapitel“ unterteilten) Informationen eingeben können. Links werden die vorhandenen, rechts die zu exportierenden Inhalte angezeigt. Sie können Inhalte via Drag & Drop verschieben, um einen benutzerdefinierten Export zu erstellen:





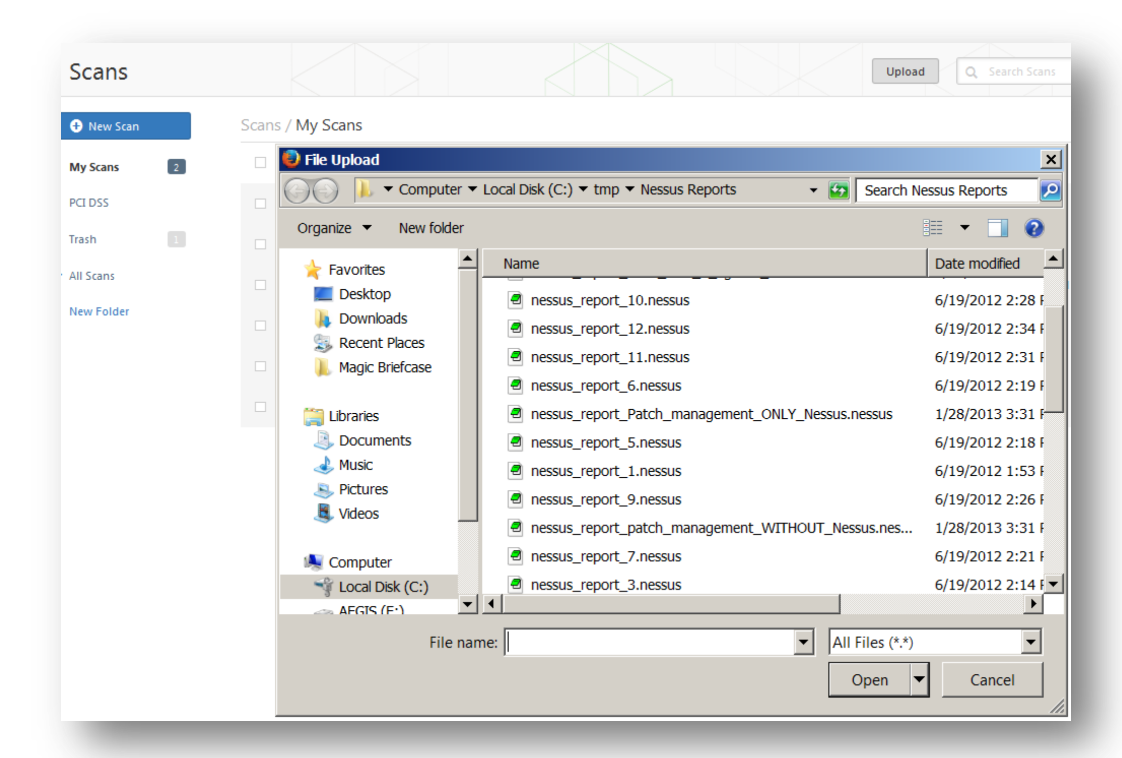
Nur mit Nessus 5 durchgeführte Compliancescans können mit Compliancekapiteln im PDF- oder HTML-Format exportiert werden. Ein Export importierter Scans aus früheren Nessus-Versionen ist in dieser Form nicht möglich.

Berichte können in verschiedenen Formaten heruntergeladen werden. Beachten Sie, dass eine Kapitelauswahl bei einigen Formaten nicht möglich ist, da diese alle Angaben enthalten.

Option	Beschreibung
`.nessus`	Dieses XML-basierte Format ist der De-facto-Standard in Nessus 4.2 und höher. Es verwendet einen erweiterten Satz XML-Tags, um das Extrahieren und Analysieren von Informationen detaillierter zu gestalten. Dieser Bericht gestattet keine Kapitelauswahl.
`.nessus` **(v1)**	Ein XML-basiertes Format, das in Nessus 3.2 bis 4.0.2 verwendet wurde. Es ist kompatibel mit Nessus 4.x und Security Center 3 und gestattet keine Kapitelauswahl.
HTML	Ein in Standard-HTML generierter Bericht, der eine Kapitelauswahl gestattet. Der Bericht wird auf einer neuen Registerkarte in Ihrem Browser geöffnet.
PDF	Ein im PDF-Format generierter Bericht, der eine Kapitelauswahl gestattet. Je nach Größe des Berichts kann die Generierung der PDF-Datei mehrere Minuten in Anspruch nehmen. Oracle Java (vormals Sun Microsystems Java) ist für die Generierung von PDF-Berichten erforderlich.
CSV	Ein Export kommagetrennter Werten (CSV) kann zum Import in eine Reihe externer Programme wie Datenbanken, Tabellenkalkulationsprogramme und mehr verwendet werden. Dieser Bericht gestattet keine Kapitelauswahl.

Nach Auswahl des gewünschten Formats wird das Standarddialogfeld „**Datei speichern**“ Ihres Browsers angezeigt, in dem Sie die Scanergebnisse an einem Speicherort Ihrer Wahl speichern können.

Klicken Sie zum Importieren eines Berichts oben auf dem Bildschirm „**Scans**“ auf „**Upload**“, um ein Fenster zur Dateisuche zu öffnen:



Wählen Sie die `.nessus`-Scandatei aus, die Sie importieren möchten, und klicken Sie auf „**Open**“ („Öffnen“). Nessus analysiert die Daten und macht sie über die Oberfläche „**Scans**“ verfügbar.

Das .nessus-Dateiformat

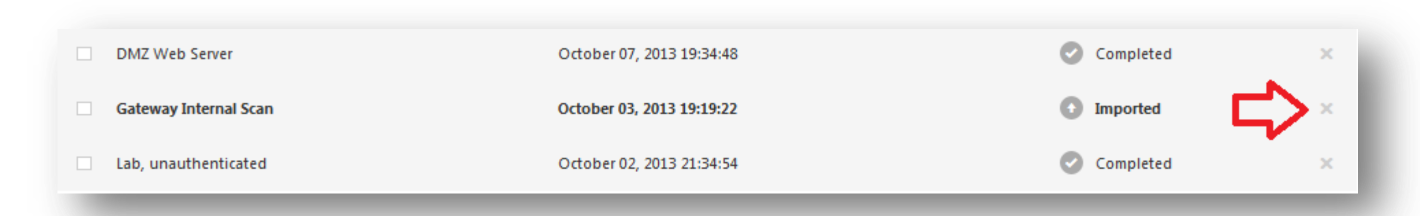
Nessus verwendet zum Exportieren und Importieren von Scans ein bestimmtes Dateiformat: das `.nessus`-Format. Dieses Format bietet die folgenden Vorteile:

- Es ist XML-basiert, d. h., es bietet Aufwärts- und Abwärtskompatibilität und ist einfach zu implementieren.
- Es ist autark, d. h., die Liste der Ziele, die vom Benutzer definierten Richtlinien und die Scanergebnisse selbst sind in einer einzigen `.nessus`-Datei enthalten.
- Es ist sicher, denn Kennwörter werden nicht in der Datei gespeichert. Stattdessen wird ein Verweis auf ein Kennwort an einem sicheren Speicherort auf dem lokalen Host abgelegt.

Der Vorgang zur Erstellung einer `.nessus`-Datei mit den Zielen, Richtlinien und Scanergebnissen beginnt mit der Einrichtung und Speicherung der Richtlinie. Danach wird die Liste mit den Zieladressen generiert und abschließend ein Scan ausgeführt. Nach Abschluss des Scans können alle Daten in einer `.nessus`-Datei gespeichert werden. Hierzu wird die Option „**Export**“ auf dem Bildschirm „**Scans**“ verwendet. Weitere Informationen zu `.nessus`-Dateien entnehmen Sie dem Dokument „Das Nessus V2-Dateiformat“.

Delete (Löschen)

Wenn Sie die Scanergebnisse nicht mehr benötigen, klicken Sie auf der Registerkarte „**Scans**“ auf das „X“ rechts neben dem Scan:





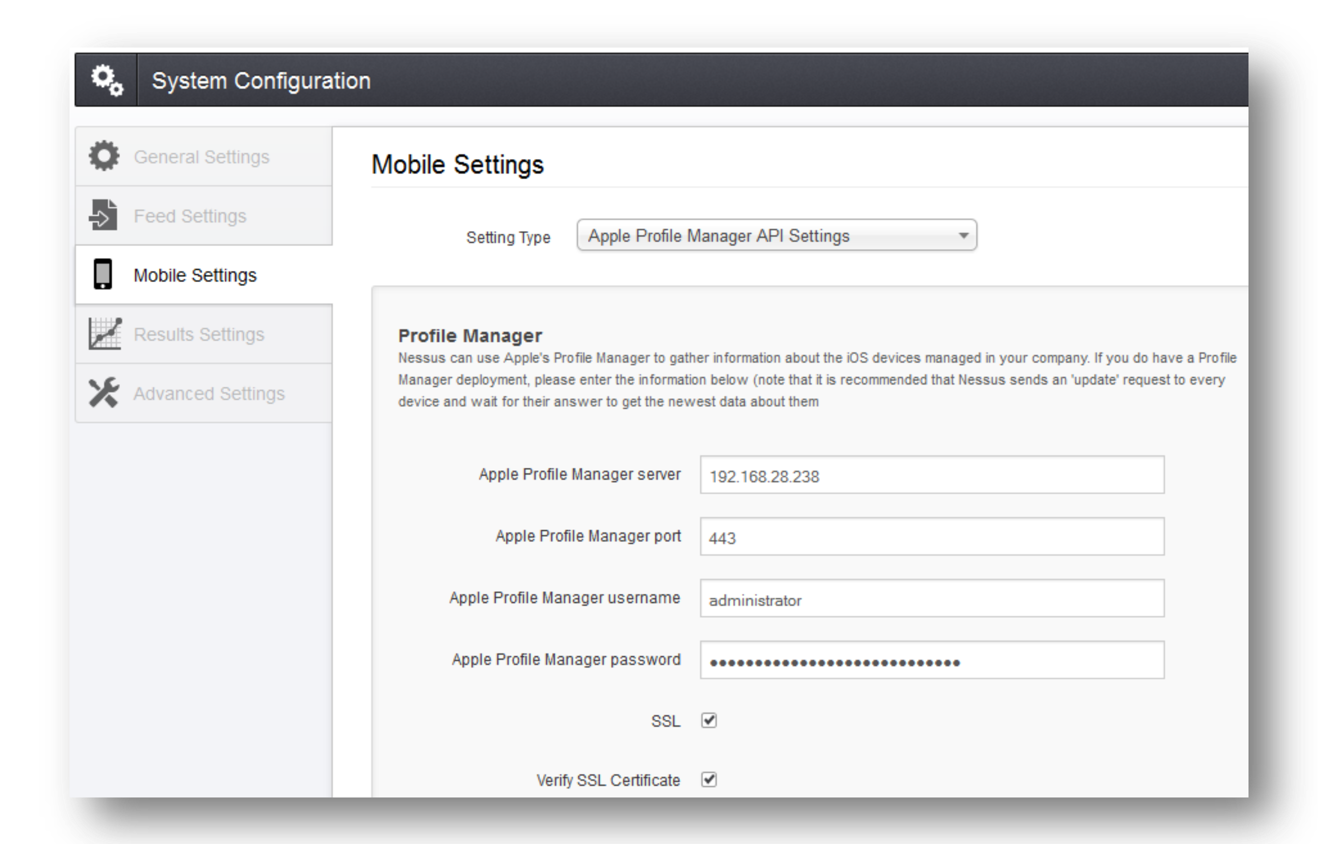
Dieser Vorgang kann nicht rückgängig gemacht werden! Wenn Sie die Scanergebnisse vor dem Löschen exportieren möchten, verwenden Sie die Funktion „**Export**“.

Mobil

Nessus 5 ist in der Lage, Active Directory Service Interfaces und den Apple Profil-Manager zu scannen. Hierdurch werden Inventar- und Sicherheitslückenscans sowohl auf Apple iOS-als auch auf Android-Geräten ermöglicht. Nessus lässt sich so konfigurieren, dass es von diesen Servern authentifiziert wird, Mobilgeräteinformationen abfragt und eventuelle Probleme auf diesen Geräten meldet.

Damit Nessus Mobilgeräte scannen kann, muss es mit Authentifizierungsangaben für die Verwaltungsserver konfiguriert werden.

Die Scanfunktion für Mobilgeräte ist im Menü „**Configuration**“ („Konfiguration“) zu finden. Auf der Registerkarte „**Mobile Settings**“ („Mobileinstellungen“) können der Apple Profil-Manager und die ADSI-Informationen konfiguriert werden. Da die Authentifizierung durch Nessus direkt auf den Verwaltungsservern stattfindet, wird automatisch eine Scanrichtlinie für Mobilgeräte erstellt, die nur die Plugin-Familie „Mobile“ umfasst. Ein entsprechender „Mobile“-Scan wird unter „**Templates**“ („Vorlagen“) eingerichtet. Mit diesem Scan können Mobilgeräte nach Bedarf gescannt werden.

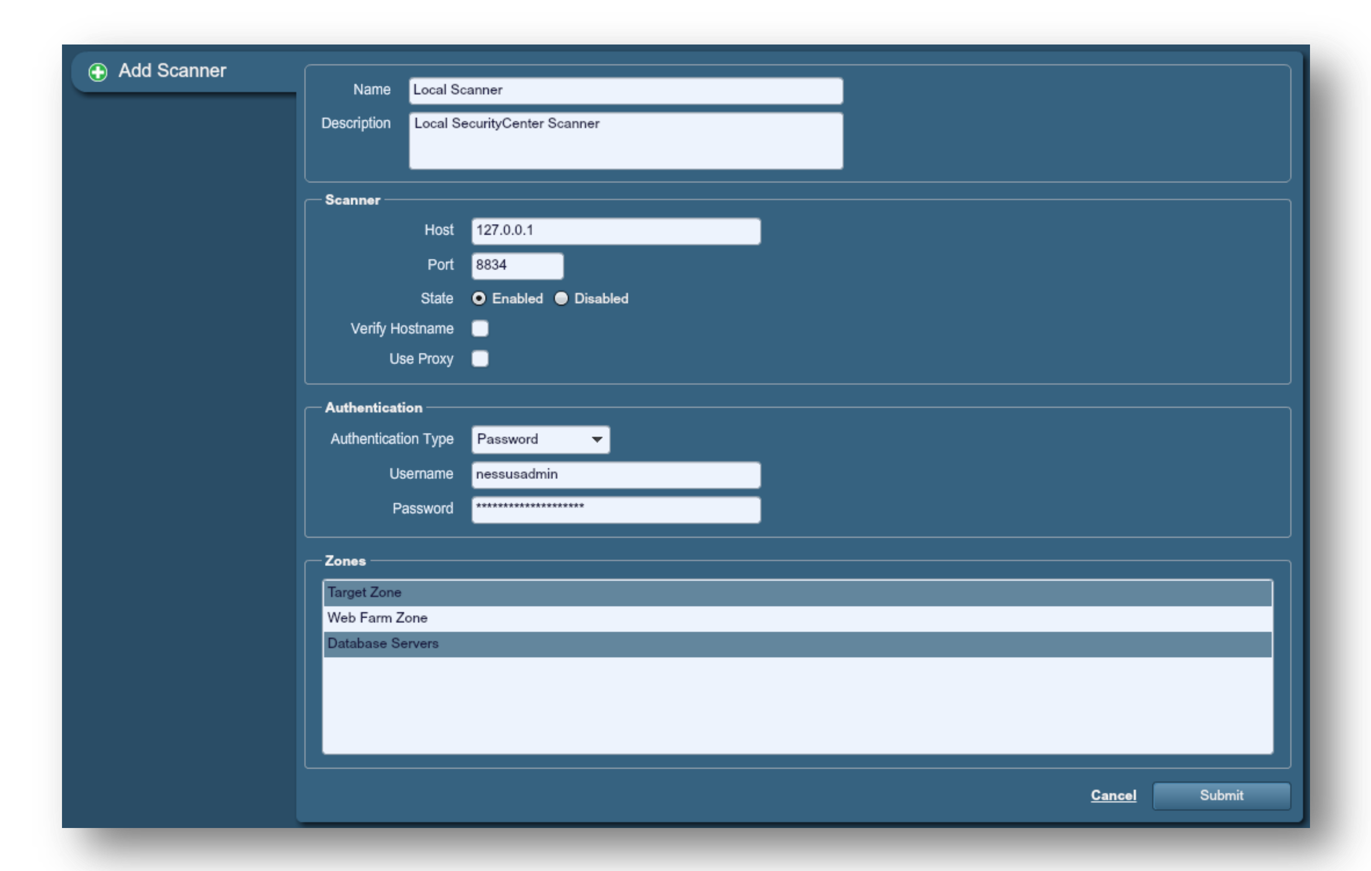


SecurityCenter

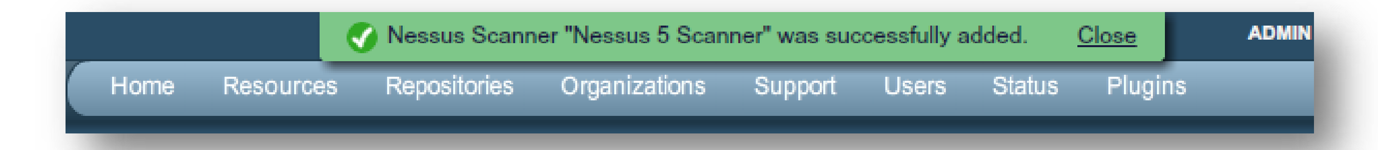
SecurityCenter für die Kooperation mit Nessus konfigurieren

Mithilfe der SecurityCenter-Verwaltungsoberfläche können Zugriff und Steuerung beliebiger Nessus-Scanner mit der Versionsnummer 4.2.x oder höher konfiguriert werden. Klicken Sie auf die Registerkarte „**Resources**" („Ressourcen") und dann auf „**Nessus Scanners**". Klicken Sie auf „**Add**" („Hinzufügen"), um das Dialogfeld „**Add Scanner**" („Scanner hinzufügen") zu öffnen. Angegeben werden müssen die IP-Adresse oder der Hostname des Nessus-Scanners, der Nessus-Port (Standard: 8834), der bei der Konfiguration von Nessus erstellte Authentifizierungstyp sowie der Anmeldename des Administrators und das zugehörige Kennwort oder die erforderlichen Zertifikatsinformationen. Die Kennwortfelder sind nicht verfügbar, wenn die Authentifizierung via SSL-Zertifikat (Option „**SSL Certificate**") ausgewählt wird. Die Funktion zur Überprüfung des Hostnamens ermöglicht die Verifizierung des CN (Common Name) im SSL-Zertifikat, das vom Nessus-Server übermittelt wurde. Der Status des Nessus-Scanners kann nach Bedarf auf „Enabled" („Aktiviert") oder „Disabled" („Deaktiviert") festgelegt werden. Zudem können die Verwendung des Proxys und eine Reihe von Scanzones ausgewählt werden, denen der Nessus-Scanner zugewiesen ist.

Nachfolgend gezeigt ist eine Bildschirmabbildung der Seite „**Add Scanner**“ aus SecurityCenter 4.7:



Nach dem erfolgreichen Hinzufügen des Scanners wird das folgende Banner angezeigt:



Weitere Informationen zur Integration von Nessus und SecurityCenter finden Sie im „SecurityCenter-Administrationshandbuch“, das über das Tenable Support Portal bezogen werden kann.

Hostbasierte Firewalls

Wenn Ihr Nessus-Server mit einer Personal Firewall wie beispielsweise Zone Alarm, BlackICE, der Windows XP Firewall oder einer anderen Firewallsoftware konfiguriert ist, müssen Verbindungsanfragen von der IP-Adresse von SecurityCenter zugelassen werden.

Standardmäßig ist der Port 8834 zur Kommunikation mit SecurityCenter vorgesehen. Auf Systemen unter Microsoft XP Service Pack 2 und höher erhält der Benutzer nach Klick auf „**Sicherheitscenter**“ in der „**Systemsteuerung**“ die Möglichkeit, die Einstellungen der Windows-Firewall zu verwalten. Um Port 8834 zu öffnen, wählen Sie die Registerkarte „**Ausnahmen**“ aus und fügen Port 8834 zur Liste hinzu.

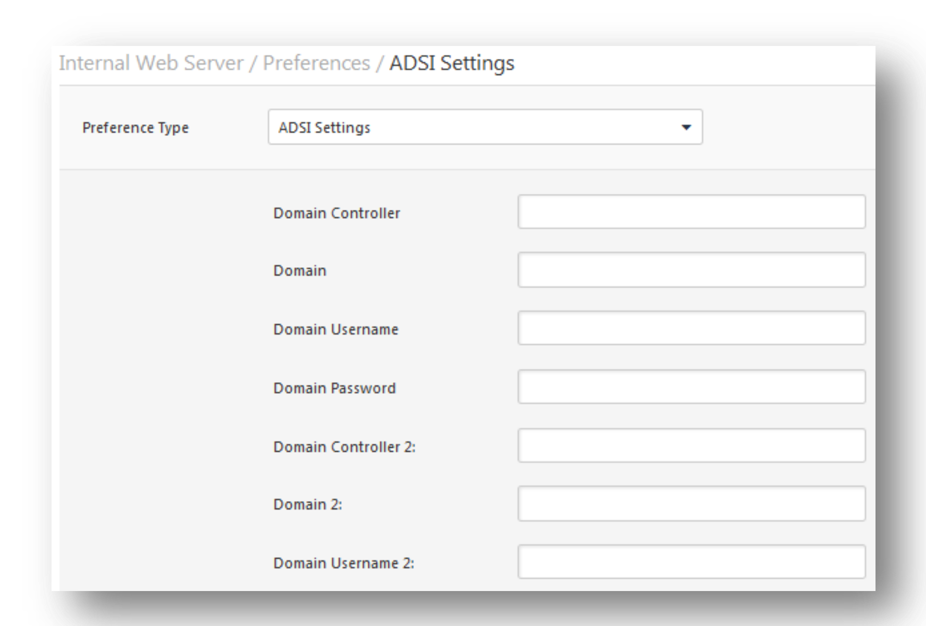
Details zu Scaneinstellungen

Die unter „**Policies**“ („Richtlinien“) gezeigte Registerkarte „**Preferences**“ („Voreinstellungen“) enthält fast 40 Dropdownmenüs, die Ihnen eine detaillierte Konfiguration der Scaneinstellungen ermöglichen. Nehmen Sie sich etwas Zeit, um die einzelnen Menüs kennen zu lernen und zu konfigurieren. Hierdurch erhalten Sie nicht nur mehr Flexibilität, sondern können auch im Vergleich zu Standardrichtlinien erheblich genauere Scanergebnisse erzielen. Im nächsten Abschnitt sind die einzelnen Optionen der Registerkarte „**Preferences**“ ausführlich beschrieben. Beachten Sie, dass die Liste der Konfigurationsoptionen dynamisch ist, d. h., sie hängt von der Nessus-Version, den Auditrichtlinien und weiteren Funktionen ab, auf die der verbundene Nessus-Scanner zugreifen kann. Ein Scanner aus der kostenpflichtigen Nessus-Version verfügt unter Umständen über anspruchsvollere Konfigurationsoptionen als ein Scanner in Nessus Home. Außerdem kann sich diese Liste ändern, wenn Plugins hinzugefügt oder geändert werden.

ADSI Settings

Über das Menü „**ADSI Settings**“ („ADSI-Einstellungen“) kann Nessus einen ActiveSync-Server abfragen, um festzustellen, ob Android- oder iOS-basierte Geräte angeschlossen sind. Nessus führt mithilfe der Anmeldedaten und Serverinformationen eine Authentifizierung auf dem Domänencontroller (d. h. nicht dem Exchange-Server) durch, um die Geräteinformationen direkt abzufragen. Für diese Funktion müssen keine Ports in der Scanrichtlinie angegeben werden. Die Einstellungen werden für Scans von Mobilgeräten benötigt. Nessus erfasst Informationen von jedem Telefon, das in den letzten 365 Tagen über ADSI aktualisiert wurde.

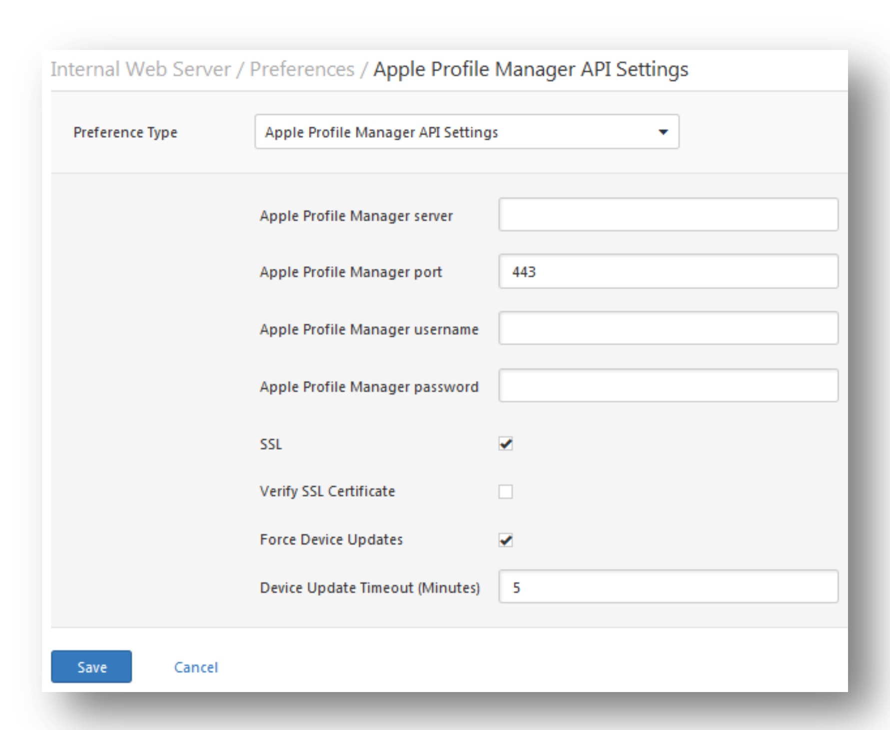
Hinweis: Hostgeräte müssen zum Abrufen von Informationen für „**ADSI Settings**“, „**Apple Profile Manager API Settings**“ und „**Good MDM Settings**“ nicht direkt gescannt werden. Der Nessus-Scanner muss den MDM-Server (Mobile Device Management) zwecks Abfrage der Informationen erreichen können. Sofern eine dieser Optionen konfiguriert wurde, erfordert die Scanrichtlinie keine Angabe zu einem zu scannenden Zielhost; auch wenn Sie „localhost“ als Ziel angeben, fragt die Richtlinie weiterhin den MDM-Server nach den Informationen ab.



Apple Profile Manager API Settings

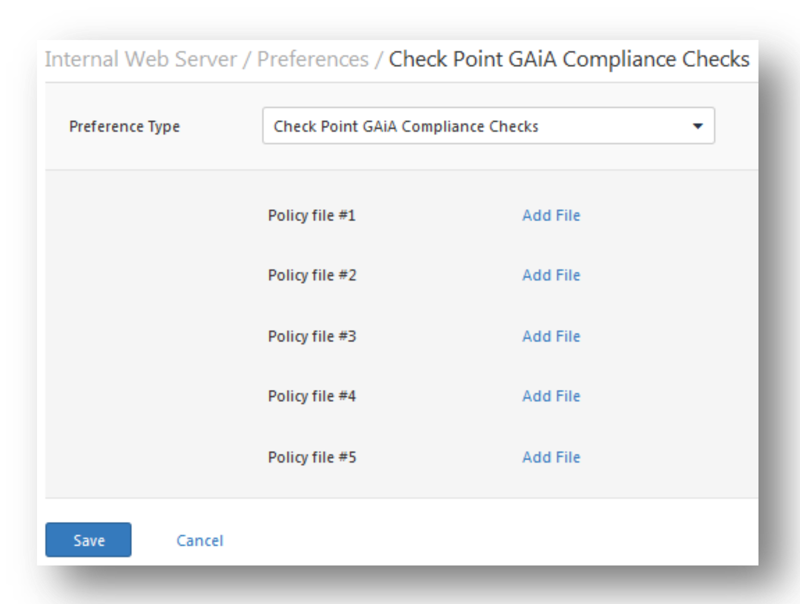
Über das Menü „**Apple Profile Manager API Settings**“ („API-Einstellungen für den Apple Profil-Manager“) fragt Nessus den Apple Profil-Manager-Server ab, um eine Enumeration der Apple iOS-Geräte (z. B. iPhone, iPad) im Netzwerk zu erstellen. Nessus führt mithilfe der Anmeldedaten und Serverinformationen eine Authentifizierung beim Profil-Manager durch, um die Geräteinformationen direkt abzufragen. Optional kann eine Kommunikation über SSL festgelegt werden, und der Server kann auch angewiesen werden, eine Aktualisierung der Geräteinformationen zu erzwingen (d. h., jedes einzelne Gerät aktualisiert seine Angaben auf dem Profil-Manager-Server).

Für diese Funktion müssen keine Ports in der Scanrichtlinie angegeben werden. Die Einstellungen werden für Scans von Mobilgeräten benötigt.



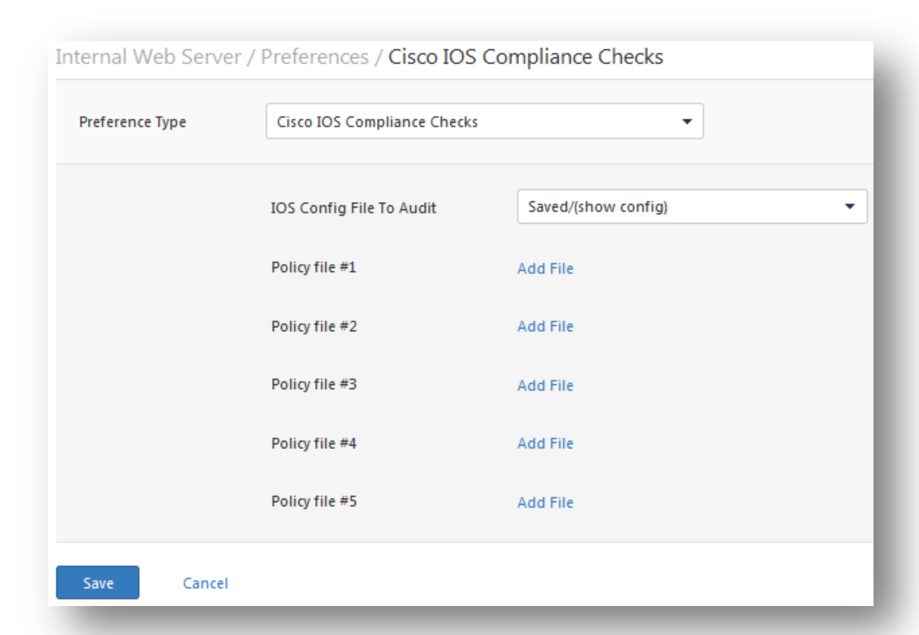
Check Point GAiA Compliance Checks

Mit dem Menü „**Check Point GAiA Compliance Checks**" („Check Point GAiA-Compliancetests") können Benutzer der kostenpflichtigen Version Richtliniendateien hochladen, anhand derer ermittelt wird, ob ein getestetes Check Point GAiA-basierendes Gerät die angeforderten Compliancestandards erfüllt. Bis zu fünf Richtlinien können gleichzeitig ausgewählt werden.



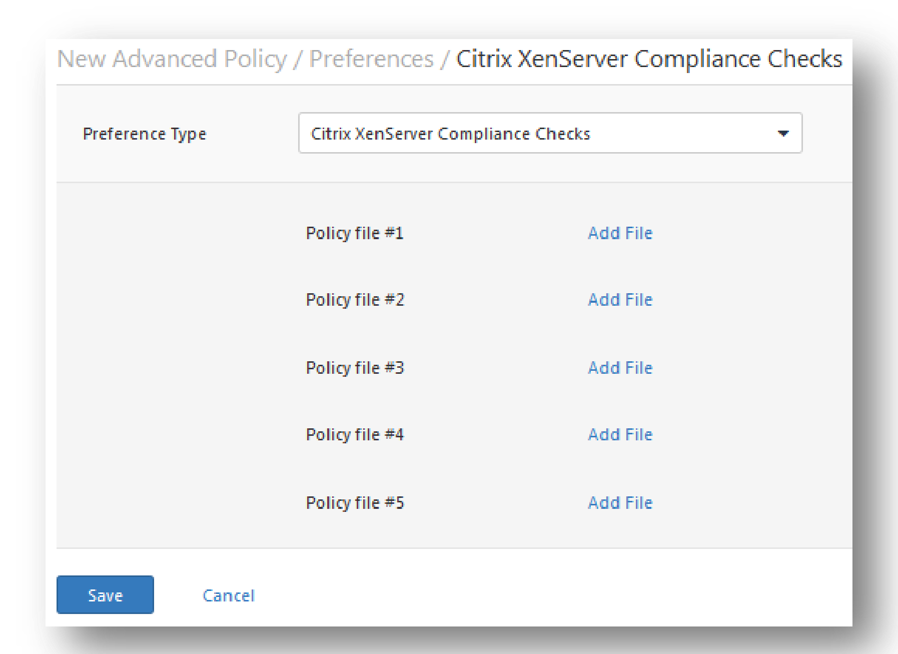
Cisco IOS Compliance Checks

Mit dem Menü „**Cisco IOS Compliance Checks**" („Cisco IOS-Compliancetests") können Benutzer der kostenpflichtigen Version Richtliniendateien hochladen, anhand derer ermittelt wird, ob ein getestetes Gerät, das unter Cisco IOS läuft, die angeforderten Compliancestandards erfüllt. Bis zu fünf Richtlinien können gleichzeitig ausgewählt werden. Diese Richtlinien können für die gespeicherte Konfiguration (Saved Config, **`show config`**), die laufende Konfiguration (Running Config, **`show running`**) oder die Startkonfiguration (Startup Config, **`show startup`**) ausgeführt werden.



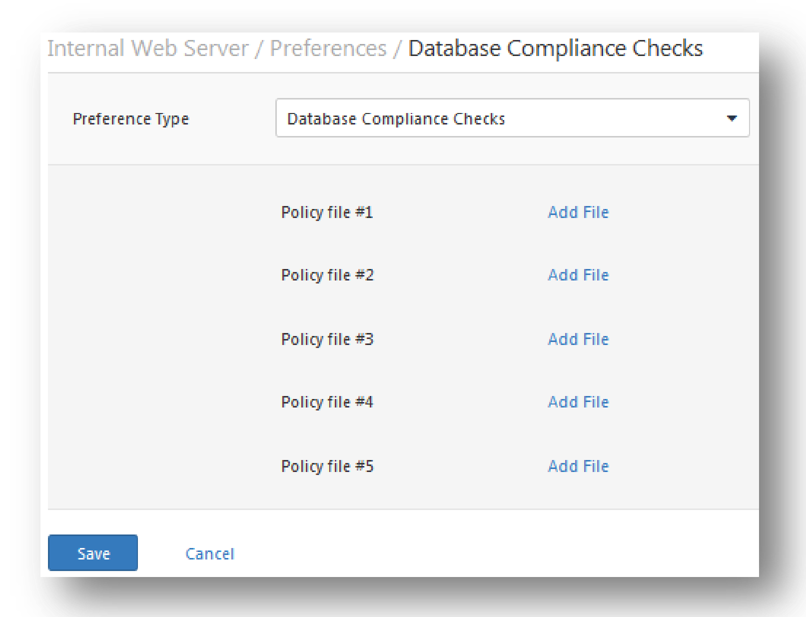
Citrix XenServer -Compliance Checks

Mit dem Menü „**Citrix XenServer Compliance Checks**" („Cisco IOS-Compliancetests") können Benutzer der kostenpflichtigen Version Richtliniendateien hochladen, anhand derer ermittelt wird, ob ein getestetes XenServer-System die angeforderten Compliancestandards erfüllt. Bis zu fünf Richtlinien können gleichzeitig ausgewählt werden.



Database Compliance Checks

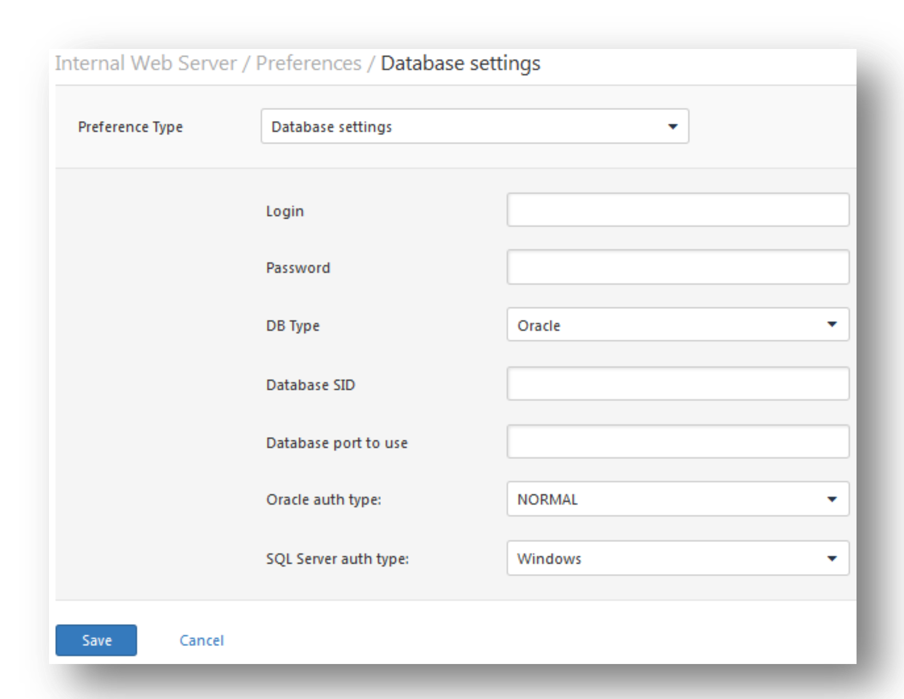
Mit dem Menü „**Database Compliance Checks**“ („Datenbank-Compliancetests“) können Benutzer der kostenpflichtigen Version Richtliniendateien hochladen, anhand derer ermittelt wird, ob eine getestete Datenbank die angeforderten Compliancestandards erfüllt. Bis zu fünf Richtlinien können gleichzeitig ausgewählt werden.



Database settings

Mithilfe der Optionen unter „**Database settings**“ („Datenbankeinstellungen“) werden der Typ der zu testenden Datenbank, zugehörige Einstellungen und Anmeldedaten angegeben:

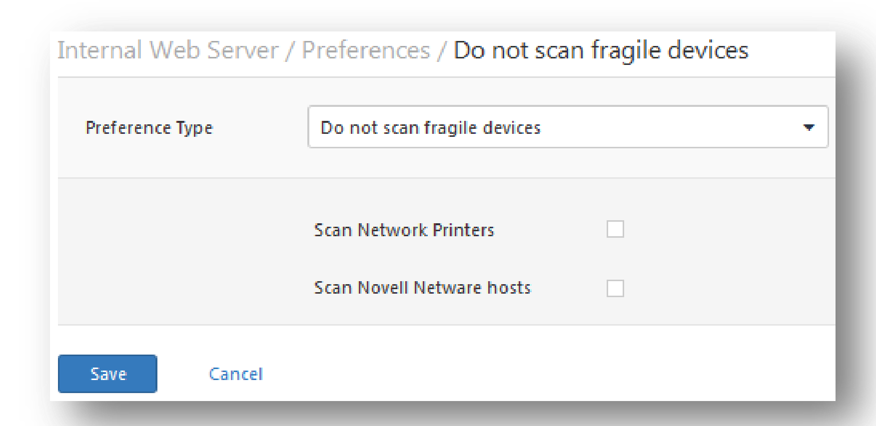
Option	Beschreibung
Login (Anmeldename)	Der Benutzername für die Datenbank.
Password (Kennwort)	Das Kennwort zum angegebenen Benutzernamen.
DB Type (Datenbanktyp)	Oracle, SQL Server, MySQL, DB2, Informix/DRDA und PostgreSQL werden unterstützt.
Database SID (System-ID der Datenbank)	ID der zu prüfenden Datenbank.
Database port to use (Zu verwendender Datenbankport)	Port, auf dem die Datenbank horcht.
Oracle auth type (Oracle-Authentifizierungstyp)	NORMAL, SYSOPER und SYSDBA werden unterstützt.
SQL Server auth type (SQL Server-Authentifizierungstyp)	Windows und SQL werden unterstützt.



Do not scan fragile devices

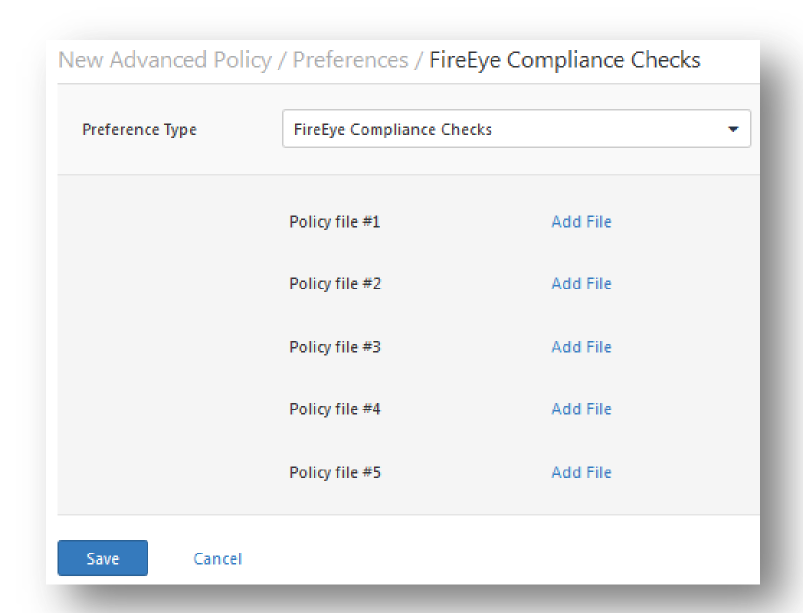
Das Menü „**Do not scan fragile devices**“ („Anfällige Geräte nicht scannen“) bietet zwei Optionen, um den Nessus-Scanner so zu konfigurieren, dass Hosts, die sich in der Vergangenheit als anfällig erwiesen haben oder bei unerwarteten

Eingaben zu Abstürzen neigen, nicht gescannt werden. Mit den Optionen „**Scan Network Printers**" („Netzwerkdrucker scannen") und „**Scan Novell Netware hosts**" („Novell Netware-Hosts scannen") kann festgelegt werden, dass diese Geräte von Nessus gescannt werden. Nessus scannt nur die Geräte, deren Optionen aktiviert wurden. Es wird empfohlen, Scans dieser Geräte auf eine Weise durchzuführen, die eine Überwachung der Systeme auf Probleme durch die IT-Mitarbeiter gestattet.



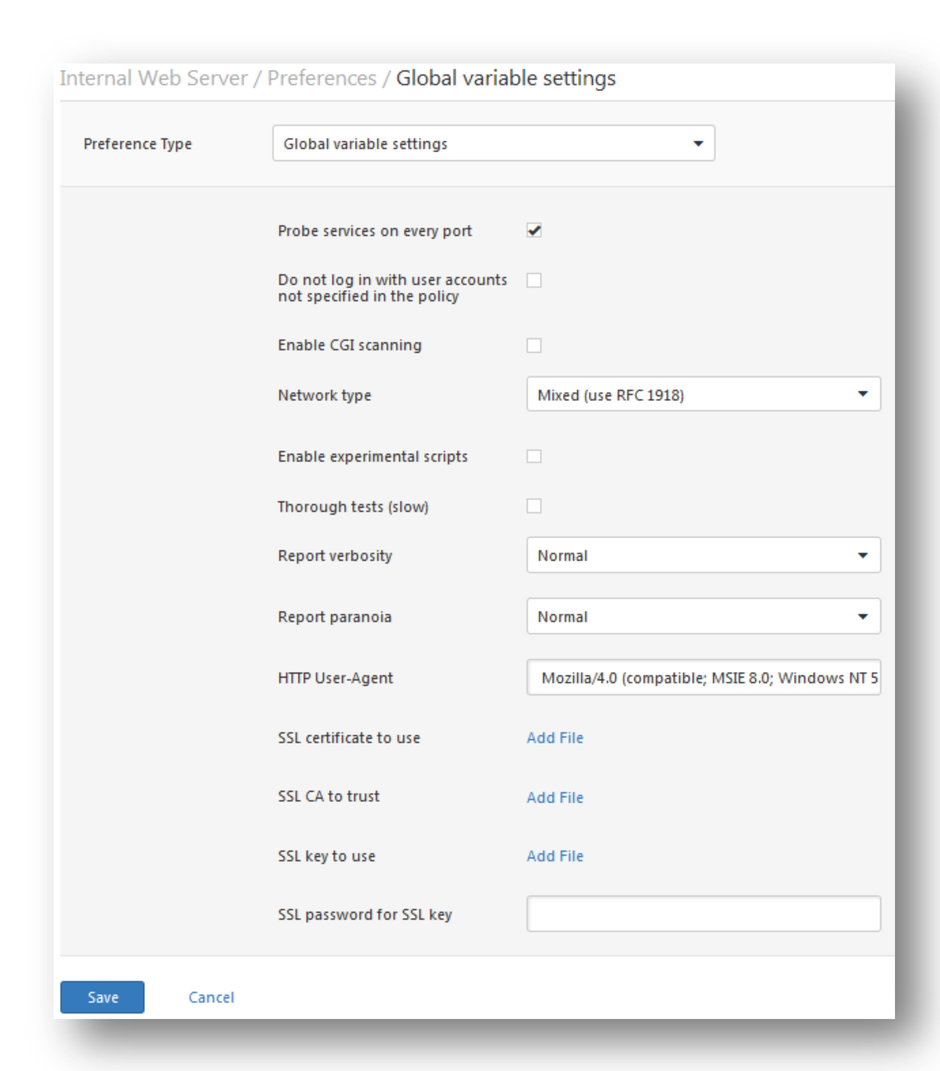
FireEye Compliance Checks

Mit dem Menü „**FireEye Compliance Checks**" („FireEye-Compliancetests") können Benutzer der kostenpflichtigen Version Richtliniendateien hochladen, anhand derer ermittelt wird, ob ein getestetes FireEye-Gerät die angeforderten Compliancestandards erfüllt. Bis zu fünf Richtlinien können gleichzeitig ausgewählt werden.



Global variable settings

Das Menü „**Global variable settings**" („Globale Variableneinstellungen") enthält eine Vielzahl von Konfigurationsoptionen für den Nessus-Server.



Die folgende Tabelle enthält ausführliche Informationen zu den verfügbaren Optionen:

Option	Beschreibung
Probe services on every port (Dienste auf jedem Port testen)	Bei Auswahl dieser Option wird versucht, jedem offenen Port den Dienst zuzuordnen, der auf diesem Port ausgeführt wird. Beachten Sie, dass es in seltenen Fällen zu Störungen einiger Dienste und zu nicht vorhersehbaren Nebeneffekten kommen kann.
Do not log in with user accounts not specified in the policy (Keine Anmeldung mit Benutzerkonten, die in der Richtlinie nicht angegeben sind)	Hiermit werden Kontensperrungen verhindert, wenn Ihre Kennwortrichtlinie vorsieht, dass Konten nach mehreren ungültigen Anmeldeversuchen gesperrt werden.

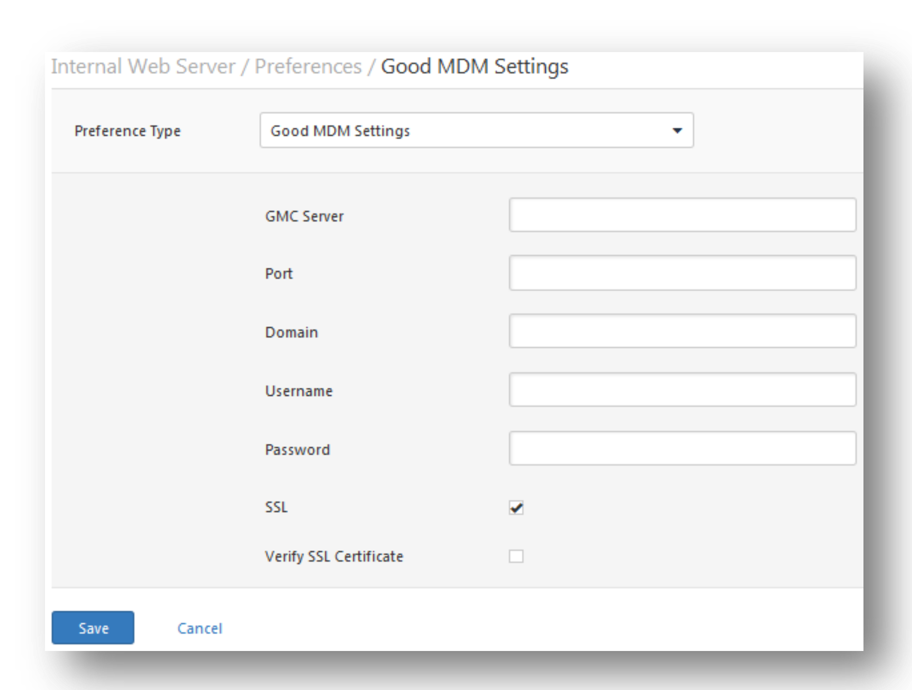
Enable CGI scanning (CGI-Scans aktivieren)	Hiermit werden CGI-Tests aktiviert. Durch Deaktivierung dieser Option wird ein Audit eines lokalen Netzwerks ganz erheblich beschleunigt.
Network type (Netzwerktyp)	Hier können Sie angeben, ob Sie öffentliche IP-Adressen, private (d. h. nicht für den Einsatz im Internet vorgesehene) IP-Adressen oder eine Kombination dieser beiden Typen verwenden. Wählen Sie „Mixed“ („Gemischt“) aus, wenn Sie RFC 1918-Adressen verwenden und mehrere Router in Ihrem Netzwerk einsetzen.
Enable experimental scripts (Experimentelle Skripts verwenden)	Gestattet die Verwendung von als experimentell betrachteten Plugins für den Scan. Lassen Sie diese Option deaktiviert, wenn Sie ein Produktionsnetzwerk scannen.
Thorough tests (slow) (Umfassende Tests, langsam)	Wenn Sie diese Option aktivieren, wird die Testleistung bestimmter Plugins erhöht. Wenn Sie beispielsweise SMB-Dateifreigaben überprüfen, wird ein entsprechendes Plugin bei aktivierter Option eine Analysetiefe von drei Stufen (statt einer Stufe) verwenden. In bestimmten Fällen kann die Auswahl dieser Option sowohl die Analyse verlängern als auch das Datenaufkommen im Netzwerk erheblich erhöhen. Beachten Sie auch, dass umfassende Scans aggressiver vorgehen und Störungen im Netzwerk wahrscheinlicher sind; dafür sind die Auditergebnisse aussagekräftiger.
Report verbosity (Berichtsausführlichkeit)	Je höher der hier zugewiesene Wert, desto mehr Informationen zu Plugin-Aktivitäten werden in den Bericht aufgenommen.
Report paranoia (Maximale Sicherheit im Bericht)	In einigen Fällen kann von Nessus remote nicht bestimmt werden, ob tatsächlich ein Schwachpunkt vorliegt. Wenn Sie für diese Optionen die Einstellung „**Paranoid**“ auswählen, wird in jedem Fall ein Schwachpunkt gemeldet, auch wenn ein Fehlalarm nicht ausgeschlossen werden kann. Umgekehrt führt die Einstellung „**Avoid false alarm**“ („ Fehlalarme vermeiden“) dazu, dass Nessus einen Schwachpunkt nicht meldet, wenn nicht sicher ist, dass er vorhanden ist. Die Standardoption („**Normal**“) stellt einen Kompromiss zwischen den vorgenannten beiden Einstellungen dar.
HTTP User-Agent	Hiermit wird angegeben, welchen Webbrowsertyp Nessus beim Scannen emuliert.
SSL certificate to use (Zu verwendendes SSL-Zertifikat)	Ermöglicht Nessus die Verwendung eines clientseitigen SSL-Zertifikats für die Kommunikation mit einem Remotehost.
SSL CA to trust (Vertrauenswürdige SSL-Zertifizierungsstelle)	Hier wird eine Zertifizierungsstelle (Certificate Authority, CA) angegeben, die Nessus als vertrauenswürdig einstuft.
SSL key to use (Zu verwendender SSL-Schlüssel)	Hiermit wird ein lokaler SSL-Schlüssel zur Verwendung für die Kommunikation mit dem Remotehost angegeben.
SSL password for SSL key (SSL-Kennwort für SSL-Schlüssel)	Hier geben Sie das Kennwort zur Verwaltung des angegebenen SSL-Schlüssels an.

Good MDM Settings

Mit dem Menü „**Good MDM Settings**“ („Good MDM-Einstellungen“) kann Nessus den Server für die Good-Mobilgeräteverwaltung abfragen, um festzustellen, ob Android- oder iOS-Geräte angeschlossen sind. Nessus führt mithilfe der Anmeldedaten und Serverinformationen eine Authentifizierung auf dem GMC-Server durch, um die Geräteinformationen direkt abzufragen. Für diese Funktion müssen keine Ports in der Scanrichtlinie angegeben werden. Die Einstellungen werden für Scans von Mobilgeräten benötigt.

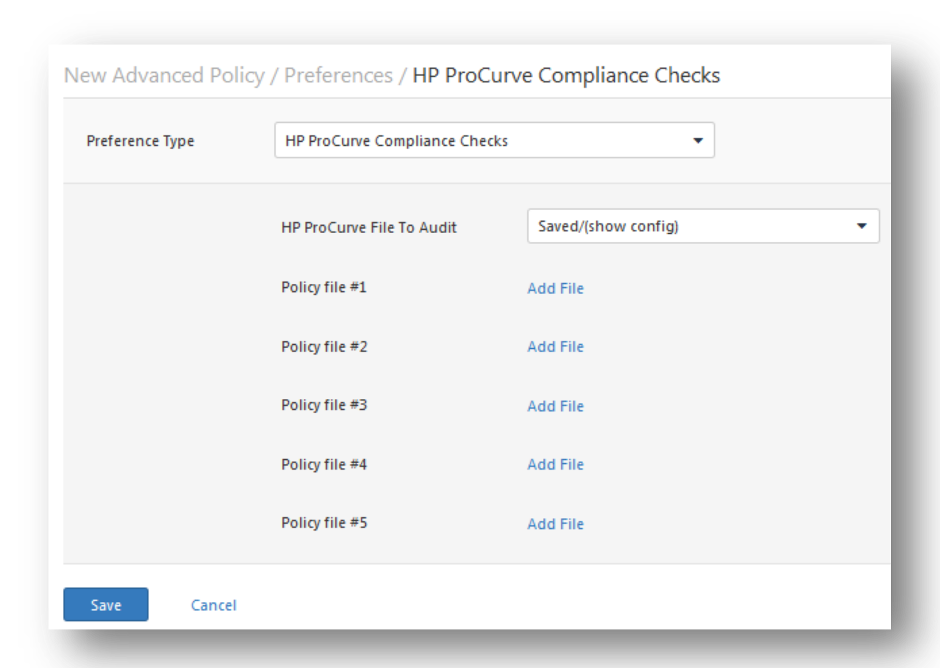
Hinweis: Hostgeräte müssen zum Abrufen von Informationen für „**ADSI Settings**“, „**Apple Profile Manager API Settings**“ und „**Good MDM Settings**“ nicht direkt gescannt werden. Der Nessus-Scanner muss den MDM-Server (Mobile Device

Management) zwecks Abfrage der Informationen erreichen können. Sofern eine dieser Optionen konfiguriert wurde, erfordert die Scanrichtlinie keine Angabe zu einem zu scannenden Zielhost; auch wenn Sie „localhost“ als Ziel angeben, fragt die Richtlinie weiterhin den MDM-Server nach den Informationen ab.



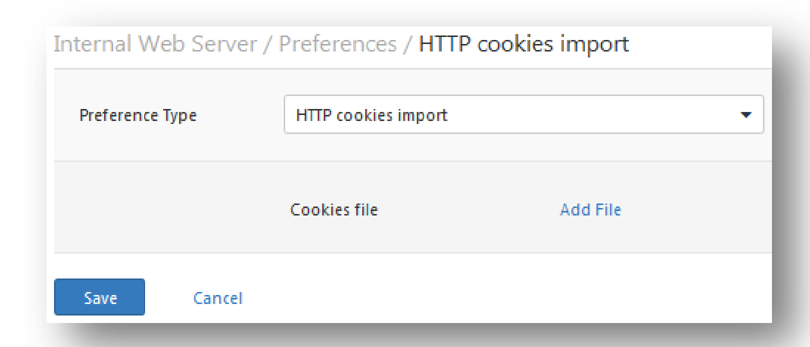
HP ProCurve Compliance Checks

Mit dem Menü „**HP ProCurve Compliance Checks**“ („HP ProCurve-Compliancetests“) können Benutzer der kostenpflichtigen Version Richtliniendateien hochladen, anhand derer ermittelt wird, ob ein getestetes HP ProCurve-Gerät die angeforderten Compliancestandards erfüllt. Bis zu fünf Richtlinien können gleichzeitig ausgewählt werden.



HTTP cookies import

Zur Erleichterung von Webanwendungstests kann Nessus HTTP-Cookies aus einer anderen Software (z. B. Webbrowser, Webproxy usw.) importieren. Der Import wird mit den Einstellungen unter „**HTTP cookies import**“ („HTTP-Cookieimport“) gesteuert. Eine Cookiedatei kann hochgeladen werden, damit Nessus die Cookies für den Zugriff auf eine Webanwendung verwendet. Die Cookiedatei muss im Netscape-Format vorliegen.

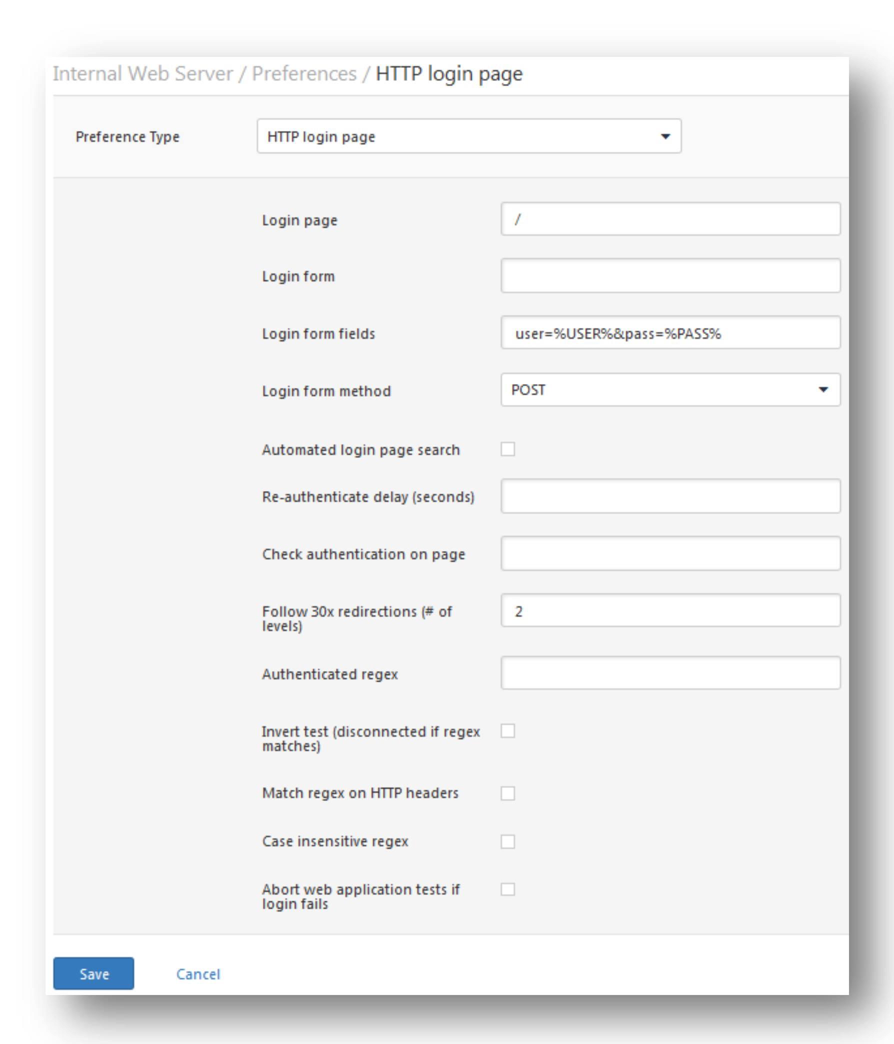


HTTP login page

Mit den Einstellungen unter „**HTTP login page**“ („HTTP-Anmeldeseite“) können Sie festlegen, an welcher Stelle authentifizierte Tests einer benutzerdefinierten webbasierten Anwendung beginnen.

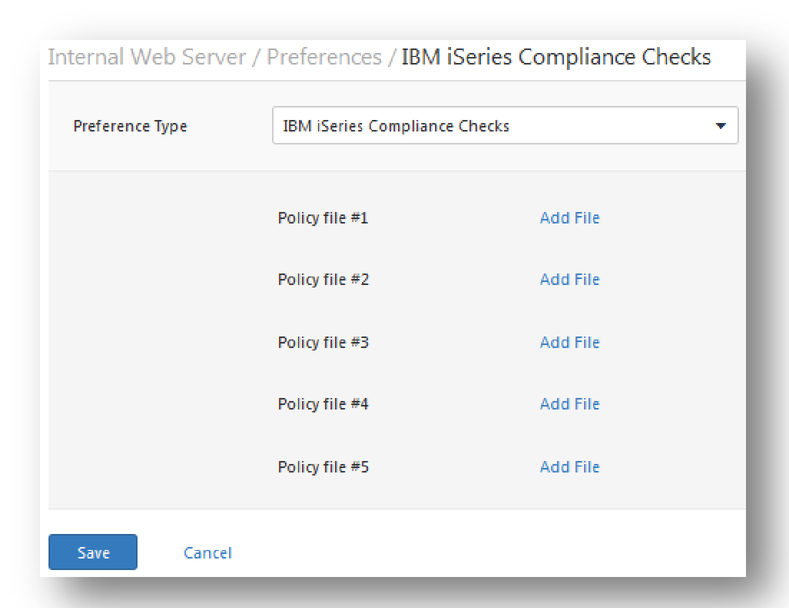
Option	Beschreibung
Login page (Anmeldeseite)	Der absolute Pfad zur Anmeldeseite der Anwendung, z. B. „/login.html“.
Login form (Anmeldeformular)	Dies ist der Parameter „action“ für die Formularmethode. Beispielsweise würde bei `<form method="POST" name="auth_form" action="/login.php">` der Wert „`/login.php`“ heißen.
Login form fields (Anmeldeformularfelder)	Geben Sie die Authentifizierungsparameter (z. B. `login=%USER%&password=%PASS%`) ein. Wenn die Schlüsselwörter %USER% und %PASS% verwendet werden, werden diese durch die Werte ersetzt, die im Dropdownmenü „Login configurations“ („Anmeldekonfiguration“) angegeben wurden. Mithilfe dieses Feldes können, falls erforderlich, auch zwei Parameter angegeben werden (z. B. ein „Gruppenname“ oder eine andere Information, die für den Authentifizierungsprozess erforderlich ist).
Login form method (Anmeldeformularmethode)	Geben Sie an, ob die Anmeldeaktion über eine GET- oder eine POST-Anforderung erfolgt.
Automated login page search (Automatische Suche der Anmeldeseite)	Hiermit wird Nessus angewiesen, nach einer Anmeldeseite zu suchen.
Re-authenticate delay (seconds) (Verzögerung für Neuauthentifizierung, in Sekunden)	Zeitliche Verzögerung bis zum nächsten Authentifizierungsversuch. Dieser Parameter ist nützlich, um das Auslösen von Schutzmechanismen gegen Brute-Force-Angriffe zu vermeiden.
Check authentication on page (Authentifizierung auf der Seite überprüfen)	Der absolute Pfad zu einer geschützten Webseite, die eine Authentifizierung erfordert (z. B. „/admin.html“). Auf diese Weise kann Nessus den Authentifizierungsstatus einfacher feststellen.

Follow 30x redirections (# of levels) (30x-Umleitungen folgen, Anzahl der Ebenen)	Wenn ein 30x-Umleitungscode von einem Webserver empfangen wird, wird hier festgelegt, ob dieser Nessus an den angegebenen Link weiterleitet.
Authenticated regex (Authentifizierter regulärer Ausdruck)	Ein regulärer Ausdruck, nach dem auf der Anmeldeseite gesucht werden soll. Manchmal ist es zur Feststellung des Sitzungsstatus nicht ausreichend, einfach nur einen 200-Antwortcode zu erhalten. Nessus kann versuchen, einen Vergleich auf Vorhandensein eines angegebenen Strings wie beispielsweise „Authentication successful!“ („Authentifizierung erfolgreich“) durchzuführen.
Invert test (disconnected if regex matches) (Test umkehren (Trennung bei Übereinstimmung mit regulärem Ausdruck))	Ein regulärer Ausdruck, nach dem auf der Anmeldeseite gesucht wird. Wenn die Suche erfolgreich ist, wird Nessus mitgeteilt, dass die Authentifizierung fehlgeschlagen ist (Beispiel: „Authentication failed!“ („Authentifizierungsfehler!“))
Match regex on HTTP headers (HTTP-Header mit regulärem Ausdruck vergleichen)	Anstelle des Datenteils einer HTTP-Antwort kann Nessus auch die Header (Kopfdaten) der Antwort nach einem gegebenen regulären Ausdruck durchsuchen, um den Authentifizierungsstatus besser ermitteln zu können.
Case insensitive regex (Keine Unterscheidung der Groß-/Kleinschreibung bei regulären Ausdrücken)	Bei Suchvorgängen mit regulären Ausdrücken wird die Groß-/Kleinschreibung standardmäßig beachtet. Mit dieser Option können Sie Nessus anweisen, die Groß-/Kleinschreibung zu ignorieren.
Abort web application tests if login fails (Bei fehlgeschlagener Anmeldung Webanwendungstests abbrechen)	Wenn die angegebenen Anmeldedaten nicht funktionieren, bricht Nessus die benutzerdefinierten Webanwendungstests ab (nicht jedoch die CGI-Plugin-Familien).


Internal Web Server / Preferences / HTTP login page
Preference Type
HTTP login page
Login page
/
Login form
Login form fields
user=%USER%&pass=%PASS%
Login form method
POST
Automated login page search
Re-authenticate delay (seconds)
Check authentication on page
Follow 30x redirections (# of levels)
2
Authenticated regex
Invert test (disconnected if regex matches)
Match regex on HTTP headers
Case insensitive regex
Abort web application tests if login fails
Save
Cancel

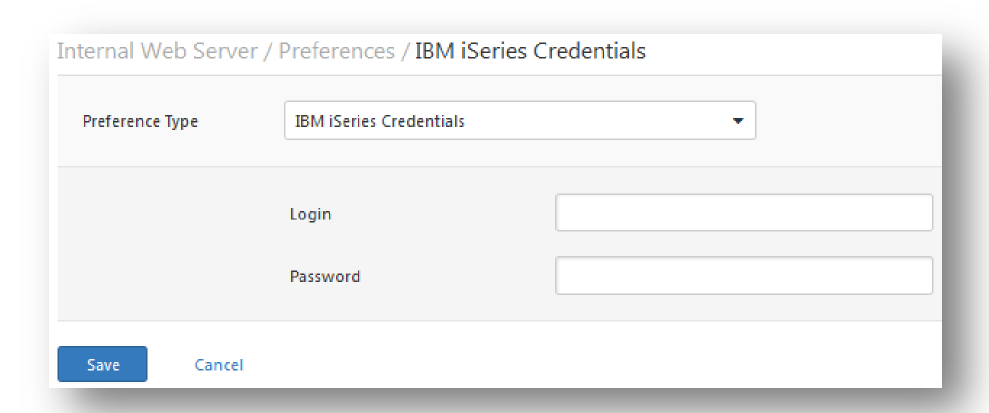
IBM iSeries Compliance Checks

Mit dem Menü „**IBM iSeries Compliance Checks**" („IBM iSeries-Compliancetests") können Benutzer der kostenpflichtigen Version Richtliniendateien hochladen, anhand derer ermittelt wird, ob ein getestetes IBM iSeries-System die angeforderten Compliancestandards erfüllt. Bis zu fünf Richtlinien können gleichzeitig ausgewählt werden.



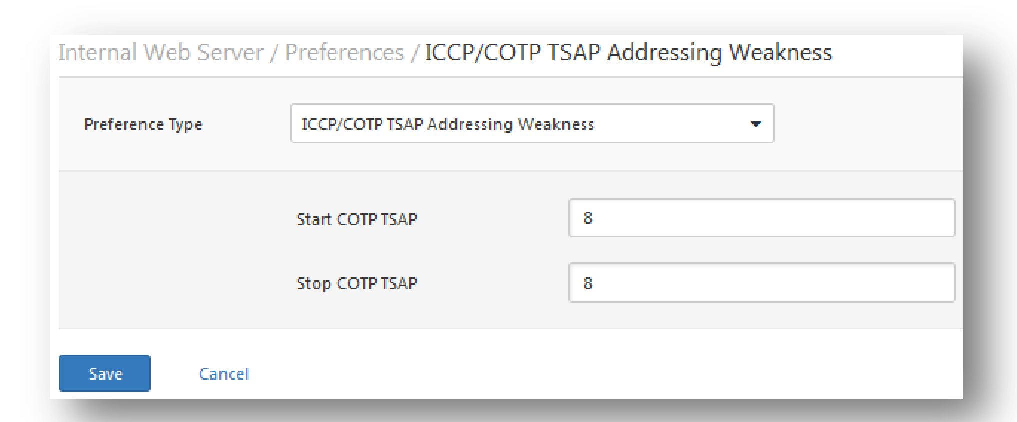
IBM iSeries Credentials

Die Einstellung „**IBM iSeries Credentials**" („IBM iSeries-Anmeldedaten") ermöglicht die Übergabe von Nessus-Anmeldedaten zur Authentifizierung bei einem IBM iSeries-System. Dies ist beispielsweise für Compliance-Audits erforderlich.



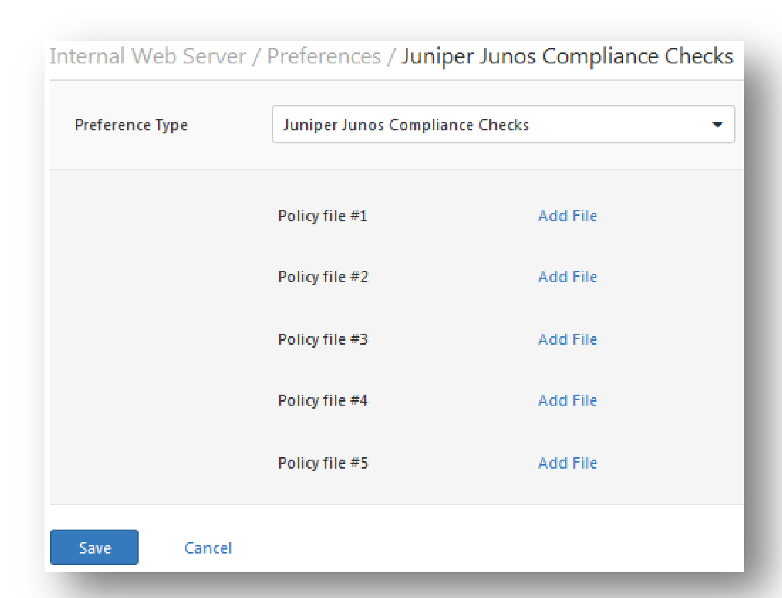
ICCP/COTP TSAP Addressing

Das Menü „**ICCP/COTP TSAP Addressing**" („ICCP/COTP-TSAP-Adressierung") dient vor allem der Konfiguration von SCADA-Tests. Es bestimmt durch Ausprobieren möglicher Werte einen COTP-TSAP-Wert (Connection Oriented Transport Protocol/Transport Service Access Points) auf einem ICCP-Server. Die Start- und Stoppwerte sind standardmäßig auf „8" festgelegt.



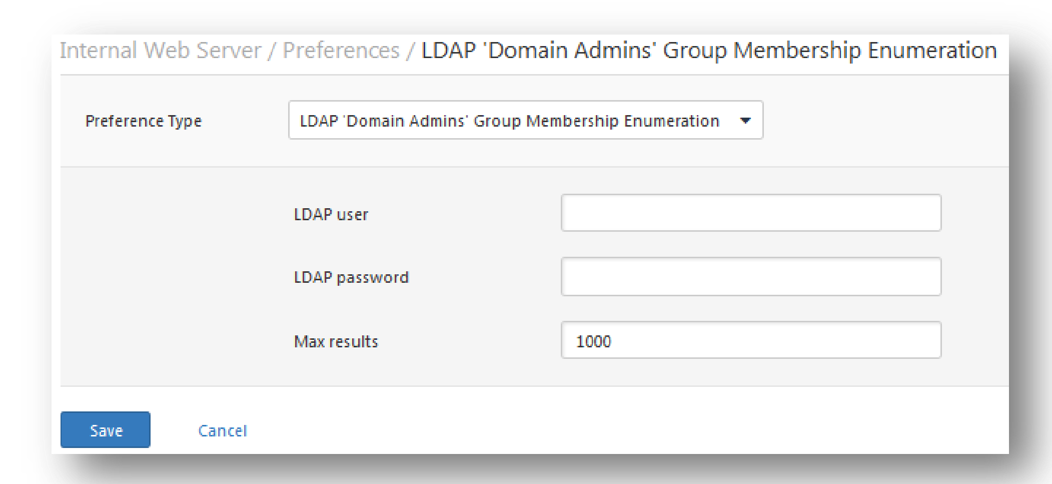
Juniper Junos Compliance Checks

Mit dem Menü „**Juniper Junos Compliance Checks**" („Juniper Junos-Compliancetests") können Benutzer der kostenpflichtigen Version Richtliniendateien hochladen, anhand derer ermittelt wird, ob ein getestetes Gerät, das unter Juniper Junos läuft, die angeforderten Compliancestandards erfüllt. Bis zu fünf Richtlinien können gleichzeitig ausgewählt werden.



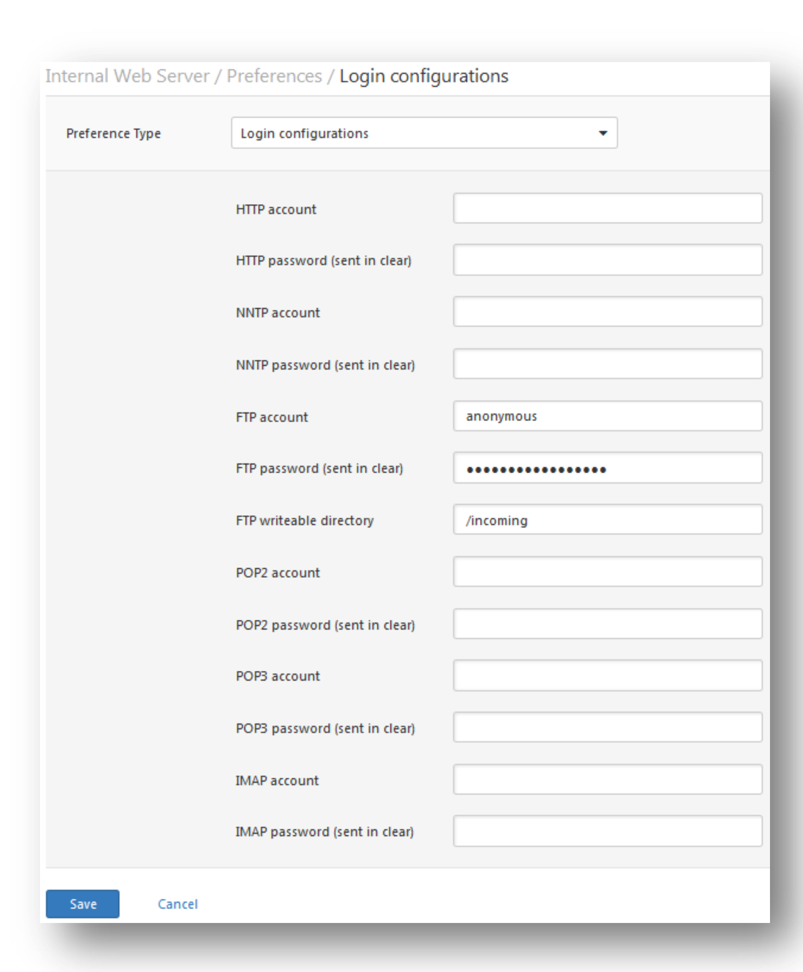
LDAP 'Domain Admins' Group Membership Enumeration

Im Menü „**LDAP 'Domain Admins' Group Membership Enumeration**" („Enumeration der Mitgliedschaften in der LDAP-Gruppe ‚Domain Admins'") können Sie LDAP-Anmeldedaten eingeben, mit denen Sie eine Liste der Mitglieder der Gruppe „Domain Admins" in einem entfernten LDAP-Verzeichnis erstellen.



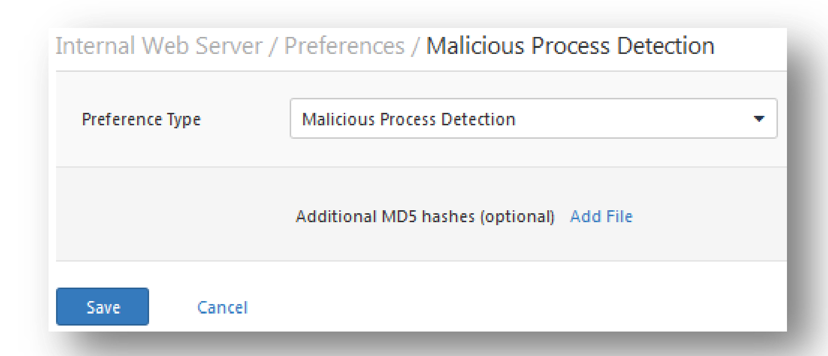
Login configurations

Im Menü „**Login configurations**“ („Anmeldekonfigurationen“) wird dem Nessus-Scanner die Verwendung von Anmeldedaten beim Testen von HTTP, NNTP, FTP, POP2, POP3 oder IMAP ermöglicht. Wenn Anmeldedaten angegeben werden, kann Nessus ausführlichere Tests zur Erkennung von Sicherheitslücken ausführen. Hier angegebene HTTP-Anmeldedaten werden nur für die Basis- und die Digest-Authentifizierung verwendet. Verwenden Sie zur Konfiguration der Anmeldedaten für eine angepasste Webanwendung das Pulldownmenü „HTTP login page“ („HTTP-Anmeldeseite“).



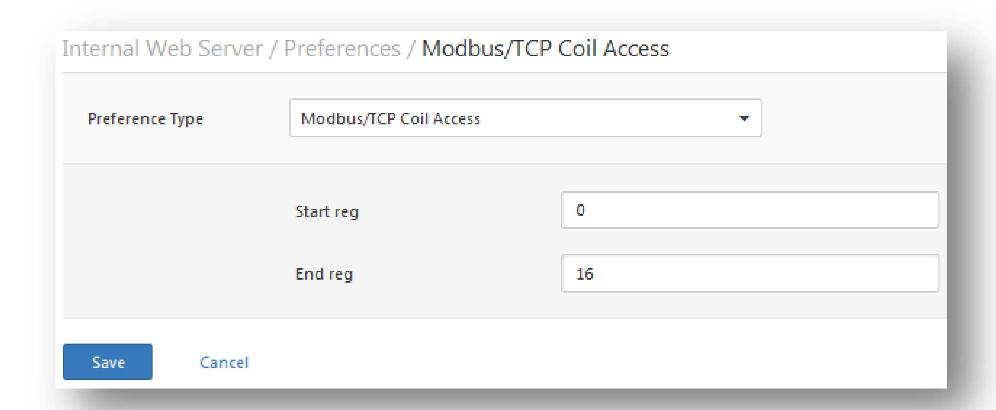
Malicious Process Detection

Im Menü „**Malicious Process Detection**“ („Erkennung bösartiger Prozesse“) können Sie eine Liste zusätzlicher MD5-Hashes angeben, die Nessus für Systemscans nach bekannter Malware verwendet. Die Liste wird vom Plugin „Malicious Process Detection: User Defined Malware Running“ („Benutzerdefinierte Malware wird ausgeführt“, Plugin-ID 65548) verwendet, das wie das Tenable-Plugin „Malicious Process Detection“ (Plugin-ID 59275) funktioniert. Zusätzliche Hashes können über eine Textdatei hochgeladen werden, die je einen MD5-Hash pro Zeile enthält. Das Hinzufügen einer Beschreibung für jeden Hash in der hochgeladenen Datei ist optional möglich. Hierzu fügen Sie die Beschreibung einfach – durch ein Komma getrennt – an den Hash an. Werden beim Scan des Ziels Übereinstimmungen gefunden, dann wird die ggf. vorhandene Beschreibung in den Scanergebnissen aufgeführt. Standardkommentare (z. B. unter Verwendung der Raute „#“) können zusätzlich zu den mit Kommata abgetrennten Beschreibungen verwendet werden.



Modbus/TCP Coil Access

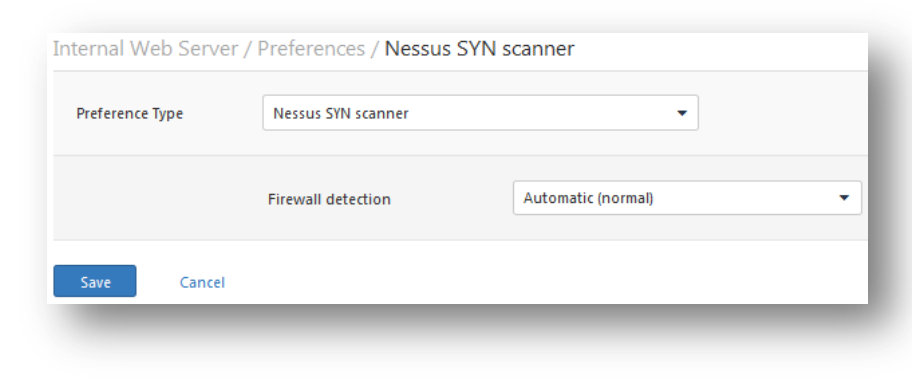
Die Optionen unter „**Modbus/TCP Coil Access**“ („Modbus-/TCP-Coil-Zugriff“) stehen nur Benutzern der kostenpflichtigen Version zur Verfügung. Dieses Dropdownmenü wird durch die SCADA-Plugins, die Bestandteil der kostenpflichtigen Version von Nessus sind, dynamisch generiert. Modbus verwendet den Funktionscode „1“ zum Auslesen der „Coils“ auf einem Modbus-Slave. Coils stellen binäre Ausgabeeinstellungen dar und sind gewöhnlich Auslösern zugeordnet. Durch Auslesen von Coils kann ein Angreifer möglicherweise ein Systemprofil erstellen und Registerbereiche erkennen, die er dann über einen Write-Coil-Befehl ändern kann. Die Standardwerte sind „0“ für das Startregister und „16“ für das Endregister.

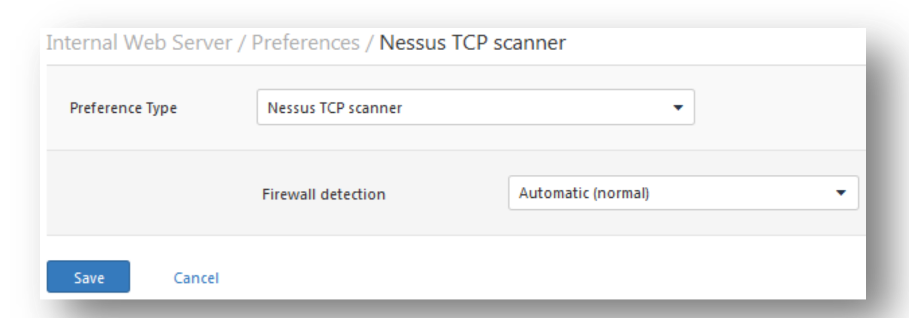


Nessus SYN-Scanner und Nessus TCP-Scanner

Mit den Optionen „**Nessus SYN scanner**“ und „**Nessus TCP scanner**“ können Sie die Erkennung einer Firewall durch die nativen SYN- bzw. TCP-Scanner verbessern.

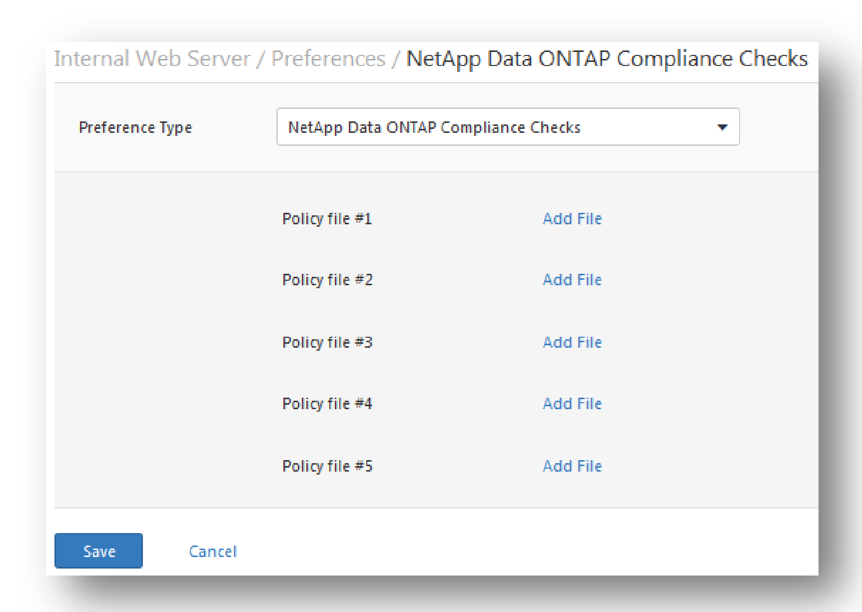
Wert	Beschreibung
Automatic (normal) (Automatisch (normal))	Durch Einstellung dieser Option kann einfacher erkannt werden, ob sich eine Firewall zwischen dem Scanner und dem Zielsystem befindet (**Voreinstellung**).
Disabled (softer) (Inaktiv (weniger aggressiv))	Hierdurch wird die Funktion **Firewall detection** („Firewallerkennung“) deaktiviert.
Do not detect RST rate limitation (soft) (RST-Häufigkeitsbeschränkung nicht erkennen (weniger aggressiv))	Hiermit wird die Möglichkeit deaktiviert, festzustellen, wie häufig Resets festgelegt werden und ob auf einem nachgeschalteten Netzwerkgerät eine Beschränkung konfiguriert ist.
Ignore closed ports (aggressive) (Geschlossene Ports ignorieren (aggressiv))	Hierbei wird versucht, Plugins auch dann auszuführen, wenn der Port geschlossen zu sein scheint. Es wird nicht empfohlen, diese Option in einem Produktionsnetzwerk einzusetzen.





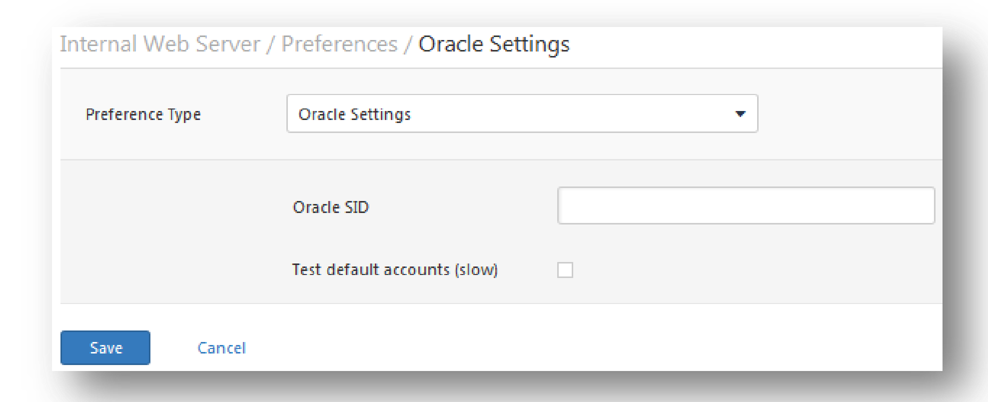
NetApp Data ONTAP Compliance Checks

Mit dem Menü „**NetApp Data ONTAP Compliance Checks**“ („NetApp Data ONTAP-Compliancetests“) können Benutzer der kostenpflichtigen Version Richtliniendateien hochladen, anhand derer ermittelt wird, ob ein getestetes NetApp Data ONTAP-Gerät die angeforderten Compliancestandards erfüllt. Bis zu fünf Richtlinien können gleichzeitig ausgewählt werden.



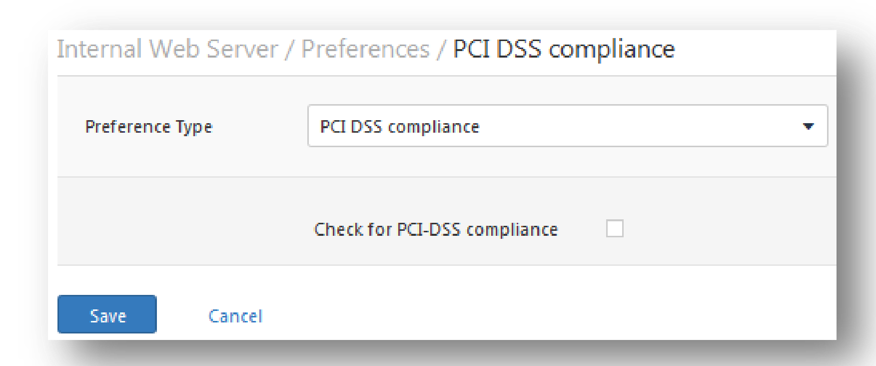
Oracle Settings

Im Menü „**Oracle Settings**“ („Oracle-Einstellungen“) wird in Nessus die Oracle Database SID konfiguriert. Außerdem wird eine Option zum Testen auf bekannte Standardkonten in der Oracle-Software hinzugefügt.



PCI DSS Compliance

Bei Auswahl der Option „**PCI DSS Compliance**" („PCI-DSS-Compliance") kann Nessus die Scanresultate mit den aktuellen Vorgaben für die PCI-DSS-Compliance vergleichen. Diese Funktion steht nur Benutzern der kostenpflichtigen Version zur Verfügung.

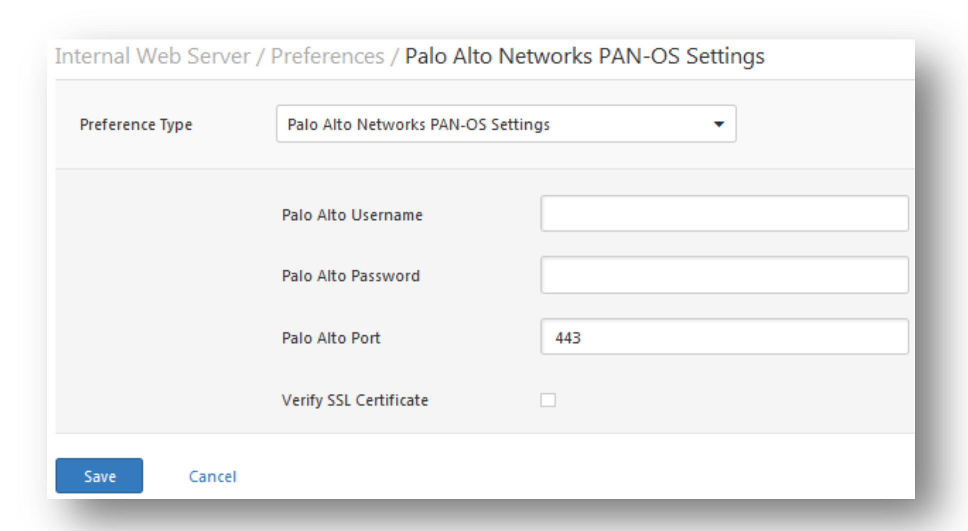


Patchmanagement

Nessus verarbeitet Anmeldedaten für die Patchmanagementsysteme Red Hat Satellite Server, WSUS, SCCM und VMware Go (vormals Shavlik), um Patch-Audits auf Systemen auszuführen, für die Nessus nicht über geeignete Anmeldedaten verfügt. Optionen für diese Patchmanagementsysteme sind in den entsprechenden Dropdownmenüs auf der Seite „Preferences" vorhanden: „**Patch Management: IBM Tivoli Endpoint Manager Server Settings**", „**Patch Management: Red Hat Satellite Server Settings**", „**Patch Management: SCCM Server Settings**", „**Patch Management: VMware Go Server Settings**" und „**Patch Management: WSUS Server Settings**". Weitere Informationen zur Verwendung von Nessus, um Hosts mithilfe dieser Patchmanagementsysteme zu scannen, entnehmen Sie dem Dokument „Patch Management Integration" („Integration des Patchmanagements").

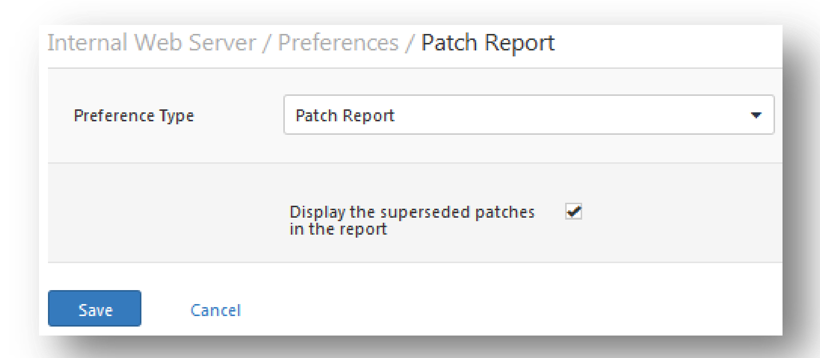
Palo Alto Networks PAN-OS Settings

Das Menü „**Palo Alto Networks PAN-OS Settings**" („Einstellungen für Palo Alto Networks PAN-OS") ermöglicht es Benutzern der kostenpflichtigen Version, Palo Alto PAN-OS-Geräte zu scannen. Dazu werden gültige Anmeldedaten benötigt, mit denen Sie den Port konfigurieren und optional das SSL-Zertifikat vollständig verifizieren können, bevor Sie fortfahren.



Patch Report

Im Menü „**Patch Report**“ (Patchbericht) können Sie Nessus so konfigurieren, dass veraltete Patchinformationen in den Scanbericht ein- bzw. aus ihm ausgeschlossen werden. Die Option ist standardmäßig aktiviert.



Ping the remote host

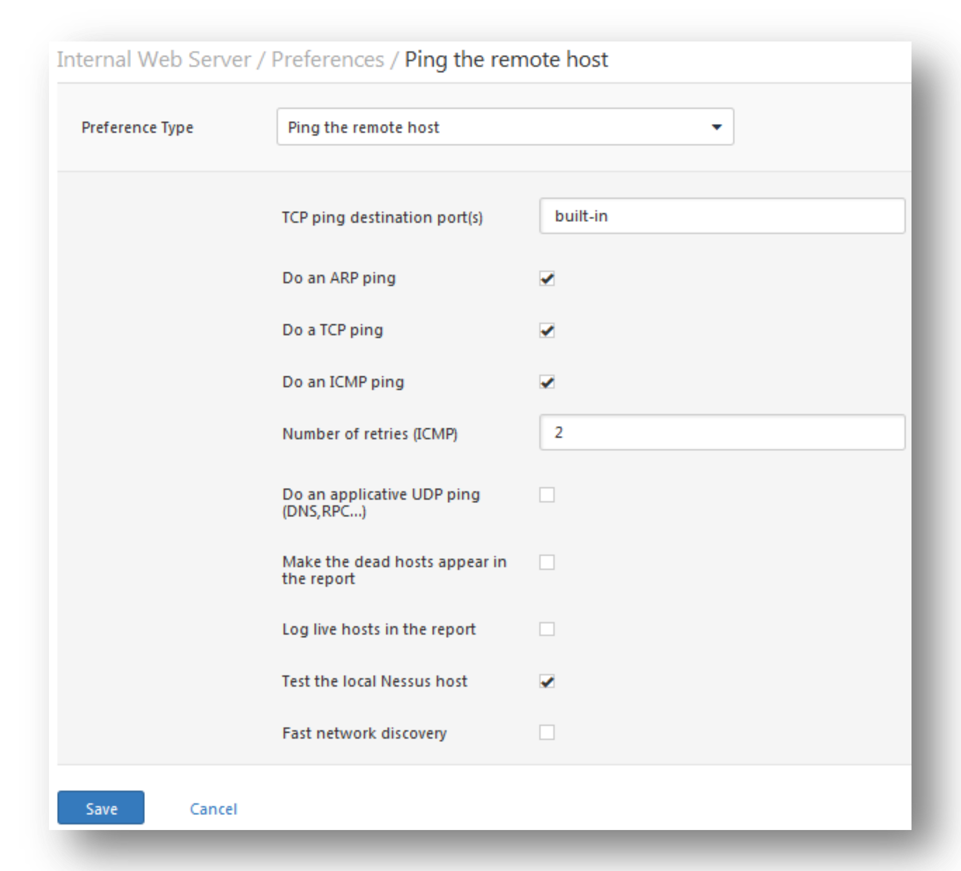
Mit den Optionen unter „**Ping the remote host**“ („Pingbefehl an Remotehost senden“) lassen sich die Funktionen zum Versenden von Pingbefehlen an Hosts durch Nessus während des Erkennungsscans sehr genau konfigurieren. Es können ARP-Pings, TCP-Pings, ICMP-Pings oder geeignete UDP-Pings verwendet werden.

Option	Beschreibung
TCP ping destination port(s) (Zielport(s) für TCP-Pings)	Gibt die Liste der Ports an, die über einen TCP-Ping überprüft werden. Wenn Sie nicht sicher sind, welche Ports Sie angeben sollen, behalten Sie die Voreinstellung „built-in“ („Integriert“) bei.
Number of Retries (ICMP) (Anzahl der Wiederholungen (ICMP))	Hiermit können Sie festlegen, wie oft die Übermittlung von Pingbefehlen an den Remotehost probiert wird. Der Standardwert ist „6“.
Do an applicative UDP ping (DNS, RPC…) (Geeigneten UDP-Ping ausführen (DNS, RPC…))	Hiermit wird ein UDP-Ping für bestimmte UDP-basierte Anwendungen wie DNS (Port 53), RPC (Port 111), NTP (Port 123) oder RIP (Port 520) ausgeführt.
Make the dead hosts appear in the report (Tote Hosts im Bericht aufführen)	Wenn diese Option aktiviert ist, werden Hosts, die auf die Pinganforderung nicht reagiert haben, als „tote“ Hosts im Sicherheitsbericht aufgeführt.
Log live hosts in the report (Hosts, die online sind, im Bericht protokollieren)	Wählen Sie diese Option aus, um im Bericht gezielt aufzuführen, an welche Remotehosts erfolgreich ein Pingbefehl gesendet werden konnte.
Test the local Nessus host (Lokalen Nessus-Host testen)	Mithilfe dieser Option können Sie den lokalen Nessus-Host in den Scan einschließen bzw. daraus ausschließen. Die Option wird angewendet, wenn der Nessus-Host in den Bereich des für den Scan konfigurierten Zielnetzwerks fällt.
Fast network discovery (Schnelle Netzwerkerkennung)	Standardmäßig werden, wenn Nessus einen Pingbefehl an eine entfernte IP-Adresse sendet und eine Antwort erhält, zusätzliche Tests durchgeführt, um sicherzustellen, dass es sich nicht um einen transparenten Proxy oder ein Lastausgleichsmodul handelt, von denen statt einer Antwort nur sinnlose Daten zurückgegeben werden (einige Geräte antworten auf jedem Port zwischen 1 und 65.535, auch wenn der betreffende Port von keinem Dienst verwendet wird). Solche Tests können

	insbesondere dann einige Zeit in Anspruch nehmen, wenn sich der Remotehost hinter einer Firewall befindet. Ist die Option „Fast network discovery“ aktiviert, dann werden diese Tests von Nessus nicht ausgeführt.



Zum Scannen von VMware-Gastsystemen muss „ping“ deaktiviert sein. Deaktivieren Sie in diesem Fall die Einträge für TCP-, ICMP- und ARP-Pings für die Sicherheitsrichtlinie „Advanced“ > „Ping the remote host“ („Erweitert“ > „Ping an Remotehost senden“).

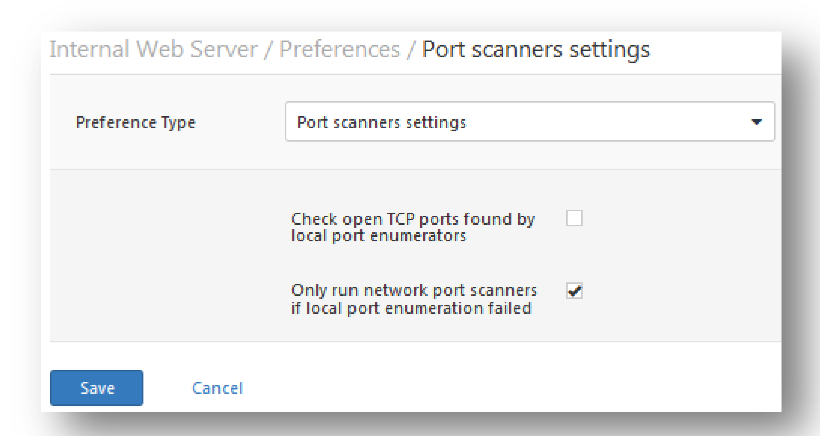


Port scanner settings

Im Menü „**Port scanner settings**“ („Portscannereinstellungen“) sind zwei Optionen für die weitere Steuerung der Portscanneraktivitäten enthalten:

Option	Beschreibung
Check open TCP ports found by local port enumerators (Offene TCP-Ports überprüfen, die von lokalen Port-Enumeratoren gefunden wurden)	Wenn ein lokaler Port-Enumerator (z. B. WMI oder netstat) einen Port erkennt, überprüft Nessus auch, ob dieser Port für Remoteverbindungen geöffnet ist. Auf diese Weise kann festgestellt werden, ob irgendeine Form der Zugriffssteuerung (z. B. TCP-Wrappers, Firewall) verwendet wird.
Only run network port scanners if local port	Andernfalls wird zunächst auf die lokale Port-Enumeration zurückgegriffen.

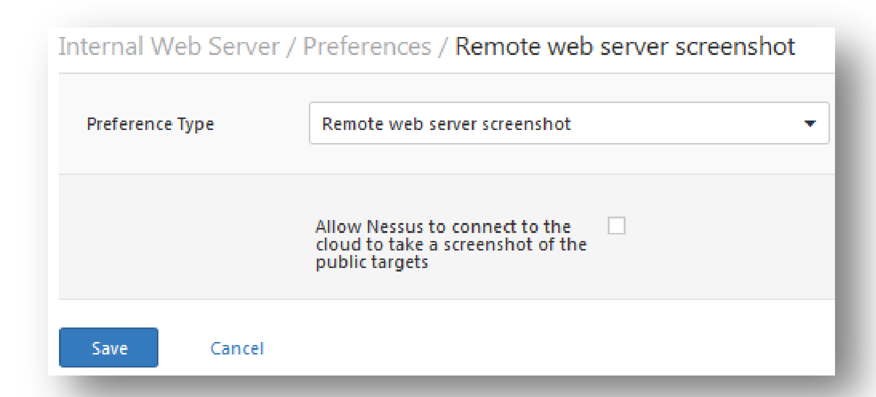
enumeration failed (Netzwerkportscanner nur ausführen, wenn die lokale Port-Enumeration fehlgeschlagen ist)	



Remote web server screenshot

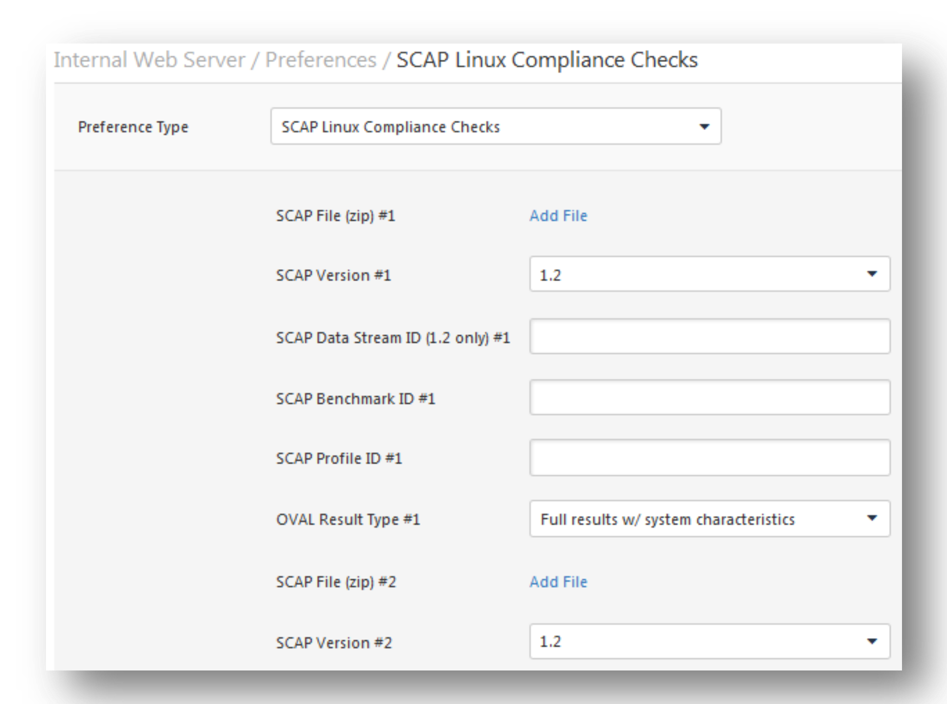
Mit dem Menü „**Remote web server screenshot**" („Screenshot des Remotewebservers") kann Nessus Screenshots zur besseren Darstellung der Resultate aufzeichnen. Dazu zählen Dienste (z. B. VNC, RDP) sowie konfigurationsspezifische Optionen (z. B. die Webserver-Verzeichnisindizierung). Die Funktion ist nur bei Hosts mit Internetverbindung funktionsfähig, da die Screenshots auf dem verwalteten Server generiert und an den Nessus-Scanner gesendet werden.

Beachten Sie, dass die Screenshots **nicht** mit einem Nessus-Scanbericht exportiert werden.



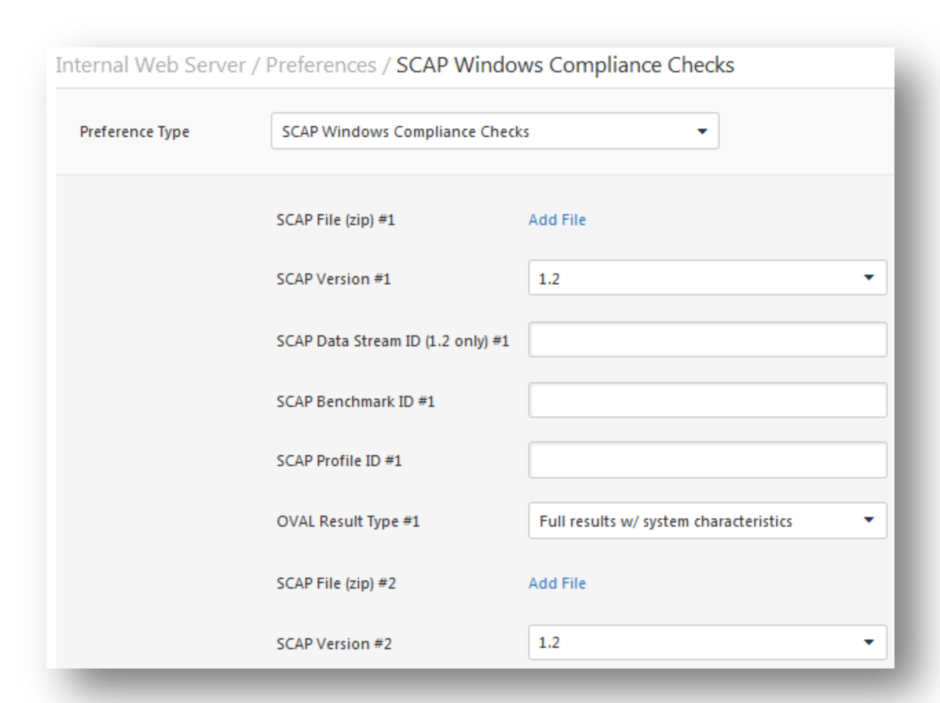
SCAP Linux Compliance Checks

Mit dem Menü „**SCAP Linux Compliance Checks**" („SCAP-Compliancetests für Linux") können Benutzer der kostenpflichtigen Version komprimierte SCAP-Dateien hochladen, anhand derer ermittelt wird, ob ein getestetes Linux-System die Compliancestandards nach SP 800-126 erfüllt. Weitere Informationen zu SCAP finden Sie auf der Website „NIST Security Content Automation Protocol".



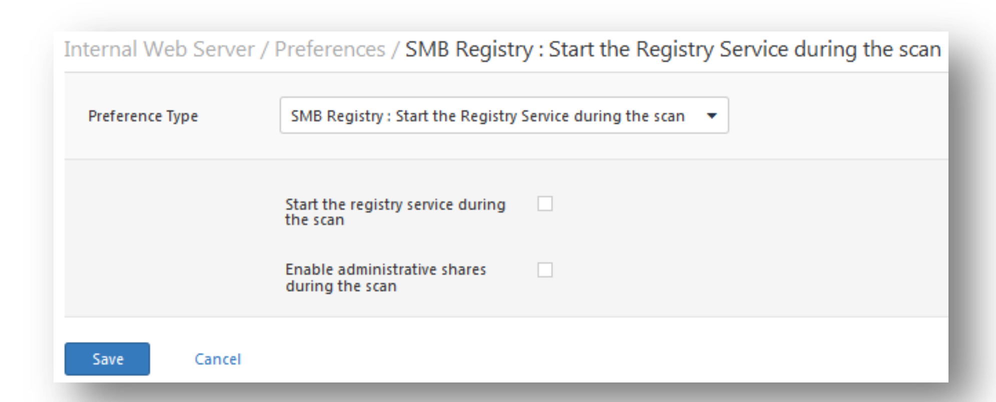
SCAP Windows Compliance Checks

Mit dem Menü „**SCAP Windows Compliance Checks**" („SCAP-Compliancetests für Windows") können Benutzer der kostenpflichtigen Version komprimierte SCAP-Dateien hochladen, anhand derer ermittelt wird, ob ein getestetes Windows-System die Compliancestandards nach SP 800-126 erfüllt. Weitere Informationen zu SCAP finden Sie auf der Website „NIST Security Content Automation Protocol".



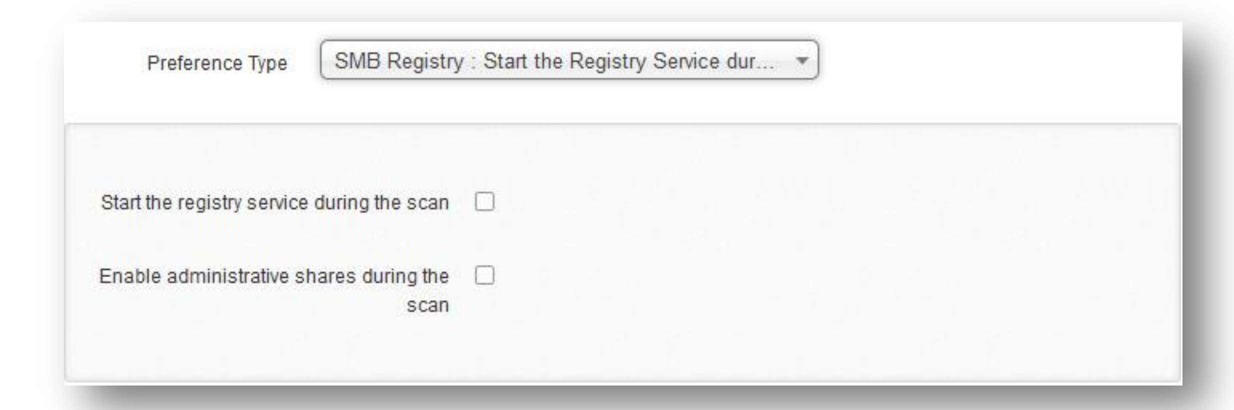
SMB Registry: Start the Registry Service During the Scan

Mit „**SMB Registry: Start the Registry Service during the scan**" („SMB-Registrierung: Registrierungsdienst während des Scans starten") kann der Dienst aktiviert werden, um einige Scanvoraussetzungen auf Computern zu erfüllen, auf denen die SMB-Registrierung nicht fortlaufend ausgeführt wird.



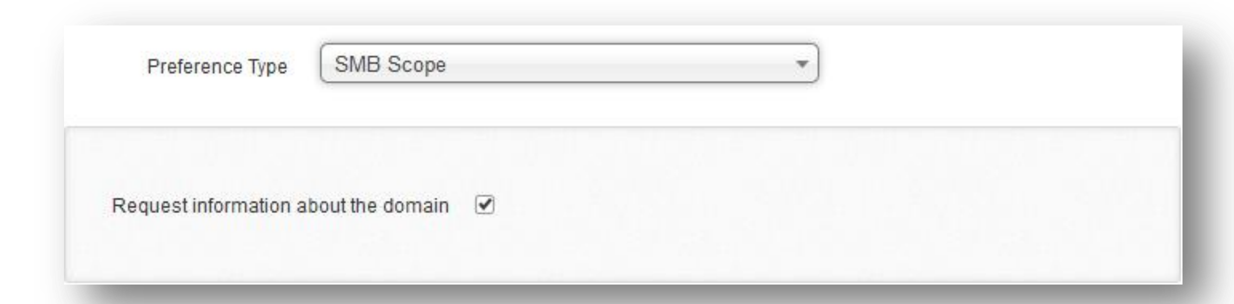
SMB Registry: Enable Administrative Shares During the Scan

Über das Menü „**SMB Registry: Enable administrative shares during the scan**" („SMB-Registrierung: Administrative Freigaben während des Scans erlauben") kann Nessus Anmeldedaten vorübergehend zum Start des SMB-Registrierungsdienstes verwenden, um weitere Audits auszuführen. Nach Abschluss deaktiviert Nessus den Dienst.



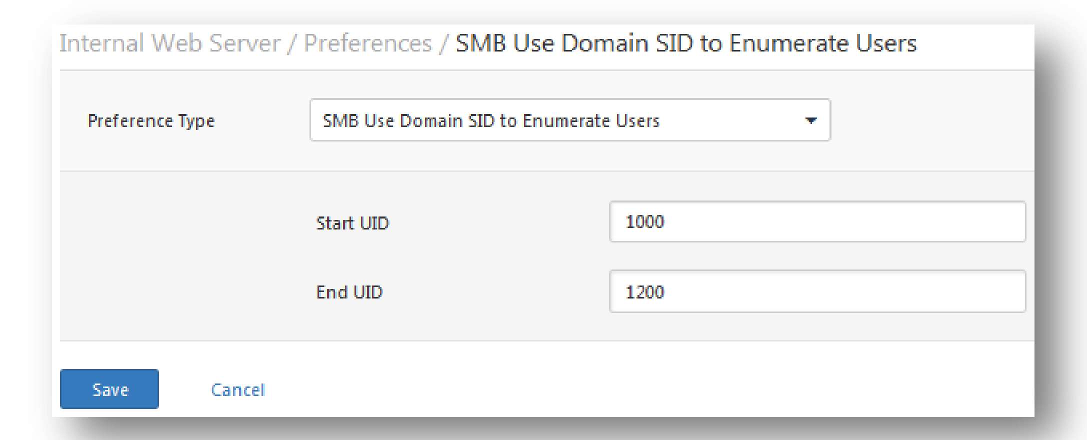
SMB Scope

Im Menü „**SMB Scope**" („SMB-Umfang") werden anstelle lokaler Benutzer Domänenbenutzer abgefragt, sofern die Option „**Request information about the domain**" („Informationen zur Domäne anfordern") festgelegt ist.



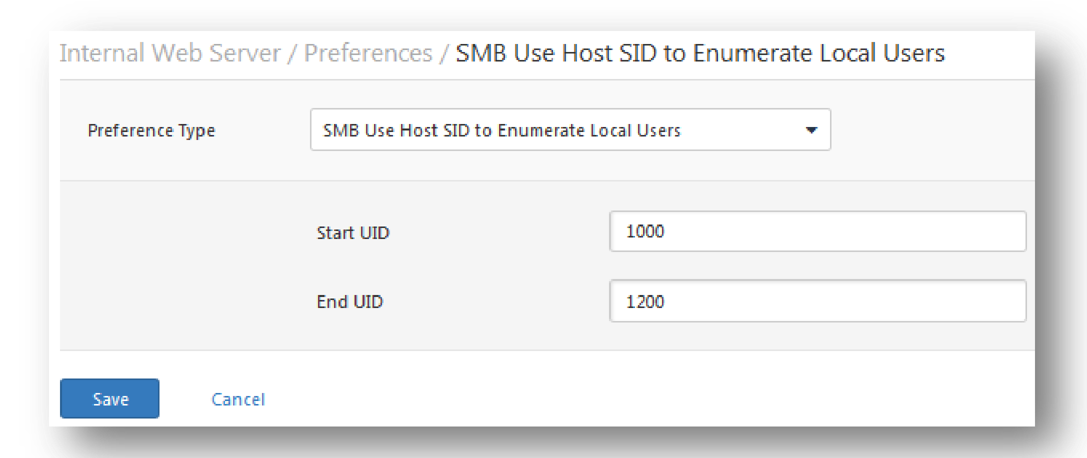
SMB Use Domain SID to Enumerate Users

Im Menü „**SMB Use Domain SID to Enumerate Users**" („Bei SMB Domänen-SID zur Enumeration von Benutzern verwenden") wird der SID-Bereich angegeben, für den eine Umkehrsuche (Reverse Lookup) von Benutzernamen in der Domäne ausgeführt wird. Für die meisten Scans wird die Standardeinstellung empfohlen.



SMB Use Host SID to Enumerate Local Users

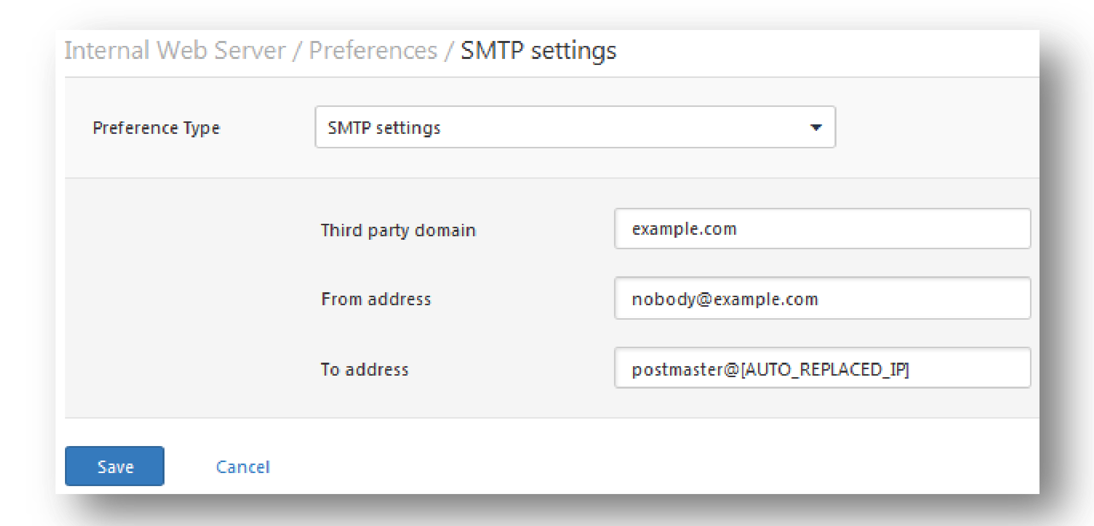
Im Menü „**SMB Use Host SID to Enumerate Local Users**" („Bei SMB Host-SID zur Enumeration von Benutzern verwenden") wird der SID-Bereich angegeben, für den eine Umkehrsuche (Reverse Lookup) lokaler Benutzernamen ausgeführt wird. Die Verwendung der Voreinstellung wird empfohlen.



SMTP settings

Im Menü „**SMTP settings**“ („SMTP-Einstellungen“) werden Optionen für SMTP-Tests (Simple Mail Transport Protocol) angegeben, die auf allen Geräten innerhalb der gescannten Domäne ausgeführt werden, auf denen SMTP-Dienste laufen. Nessus versucht dabei, Meldungen über das Gerät an die unter „**Third party domain**“ („Fremddomäne“) angegebene Fremddomäne weiterzuleiten. Wird die an die „**Third party domain**“ gesendete Nachricht von der im Feld „**To address**“ („Empfängeradresse“) angegebenen Adresse abgewiesen, dann ist der Spamversuch fehlgeschlagen. Wird die Nachricht hingegen akzeptiert, dann wurde der SMTP-Server erfolgreich zur Weiterleitung von Spam verwendet.

Option	Beschreibung
Third party domain (Fremddomäne)	Nessus versucht, Spam über jedes SMTP-Gerät an die in diesem Feld aufgeführte Adresse zu schicken. Die Adresse dieser Fremddomäne muss außerhalb des Bereichs der Site liegen, die gescannt wird bzw. den Scan ausführt. Andernfalls wird der Test durch den SMTP-Server abgebrochen.
From address (Absenderadresse)	Die an den oder die SMTP-Server gesendeten Testnachrichten geben vor, von der in diesem Feld angegebenen Adresse zu stammen.
To address (Empfängeradresse)	Nessus versucht, Nachrichten an die in diesem Feld aufgeführte Empfängeradresse zu schicken. Vorgegeben ist die Adresse **postmaster**, da sie auf den meisten Mailservern gültig ist.

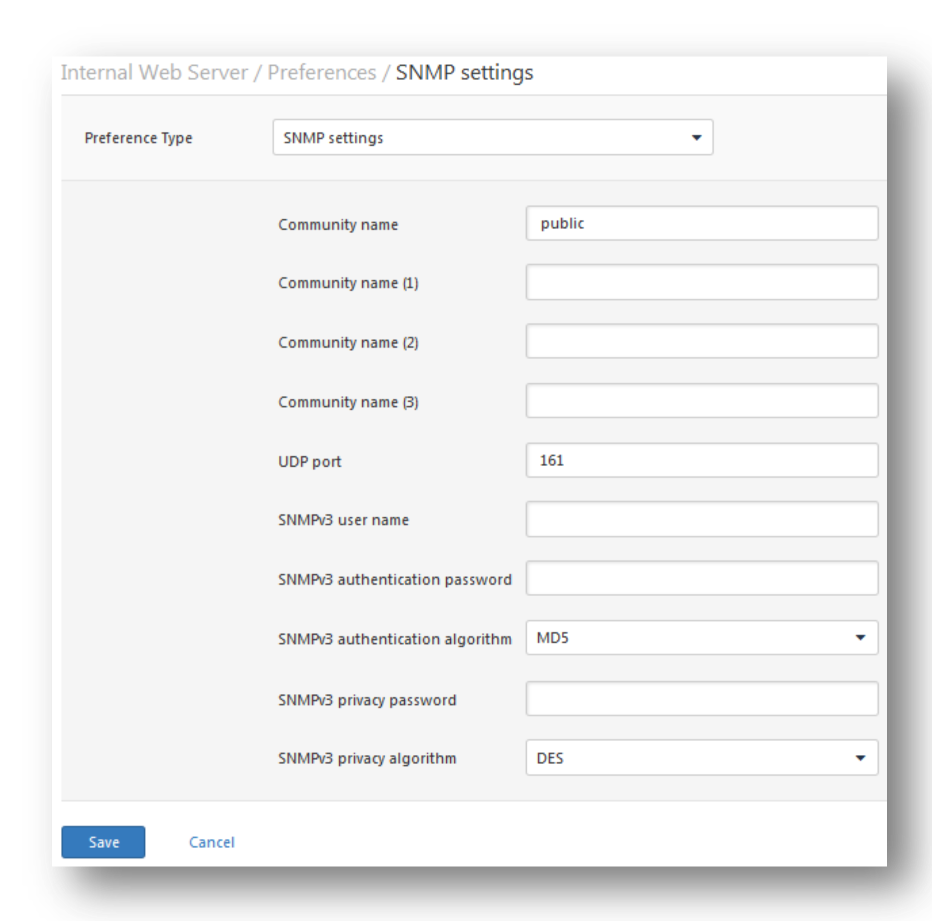


SNMP settings

Im Menü „**SNMP settings**“ („SNMP-Einstellungen“) können Sie Nessus für die Herstellung einer Verbindung mit und die Authentifizierung beim SNMP-Dienst auf dem Zielsystem konfigurieren. Im Verlauf des Scans wird Nessus einige Versuche durchführen, den Community-String zu erraten und für nachfolgende Tests zu verwenden. Je Scanrichtlinie werden bis zu vier separate Community-Strings unterstützt. Kann Nessus den Community-String und/oder das Kennwort nicht erraten, dann kann kein vollständiges Audit des Dienstes ausgeführt werden.

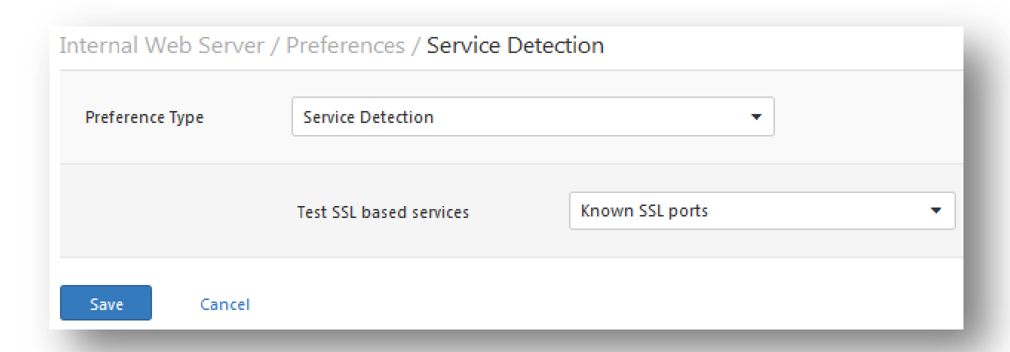
Option	Beschreibung
Community name (0-3) (Community-Name (0-3))	SNMP-Community-Name.

UDP port (UDP-Port)	Weist Nessus an, den Scan über einen anderen Port auszuführen. Vorgesehen für Fälle, in denen SNMP über einen anderen Port als 161 ausgeführt wird.
SNMPv3 user name (SNMPv3-Benutzername)	Benutzername eines SNMPv3-Kontos.
SNMPv3 authentication password (SNMPv3-Authentifizierungskennwort)	Das Kennwort zum angegebenen Benutzernamen.
SNMPv3 authentication algorithm (SNMPv3-Authentifizierungsalgorithmus)	Wählen Sie je nach vom Remotedienst unterstützten Algorithmus MD5 oder SHA1 aus.
SNMPv3 privacy password (SNMPv3-Datenschutzkennwort)	Kennwort, mit dem die verschlüsselte SNMP-Kommunikation geschützt wird.
SNMPv3 privacy algorithm (SNMPv3-Datenschutzalgorithmus)	Der für den SNMP-Datenverkehr verwendete Verschlüsselungsalgorithmus.



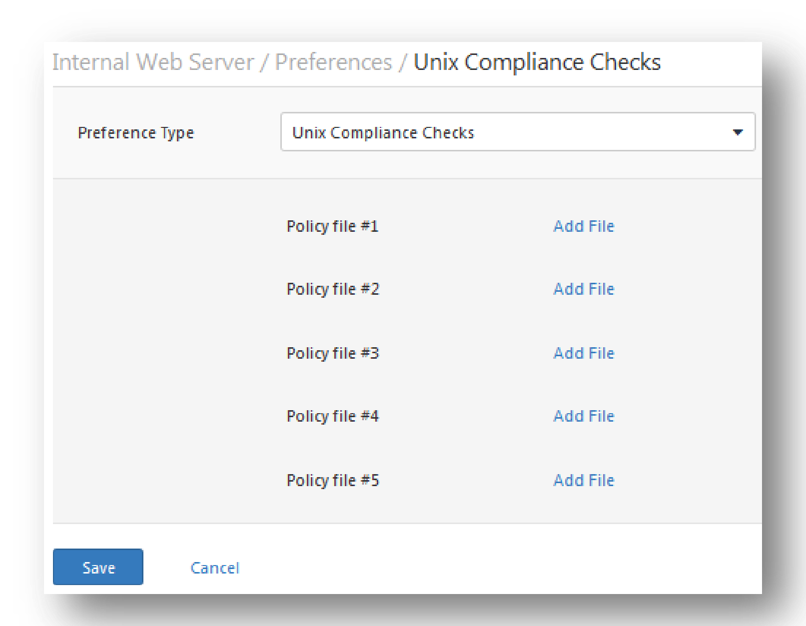
Service Detection

Über das Menü „**Service Detection**" („Diensterkennung") wird gesteuert, wie Nessus SSL-Dienste testet. Hier können Sie festlegen, ob die Tests für bekannte SSL-Ports (z. B. 443), alle Ports oder gar nicht ausgeführt wird. Das Testen der SSL-Funktionalität auf allen Ports kann auf dem getesteten Host zu einer Betriebsunterbrechung führen.



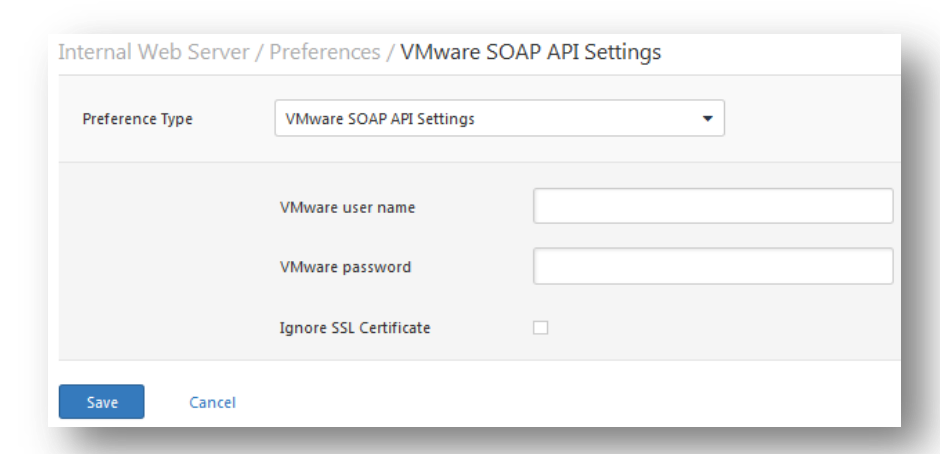
Unix Compliance Checks

Das Menü „**Unix Compliance Checks**" („UNIX-Compliancetests") ermöglicht es Benutzern der kostenpflichtigen Version, UNIX-Auditdateien hochzuladen, anhand derer ermittelt wird, ob ein getestetes System die angeforderten Compliancestandards erfüllt. Bis zu fünf Richtlinien können gleichzeitig ausgewählt werden.



VMware SOAP API Settings

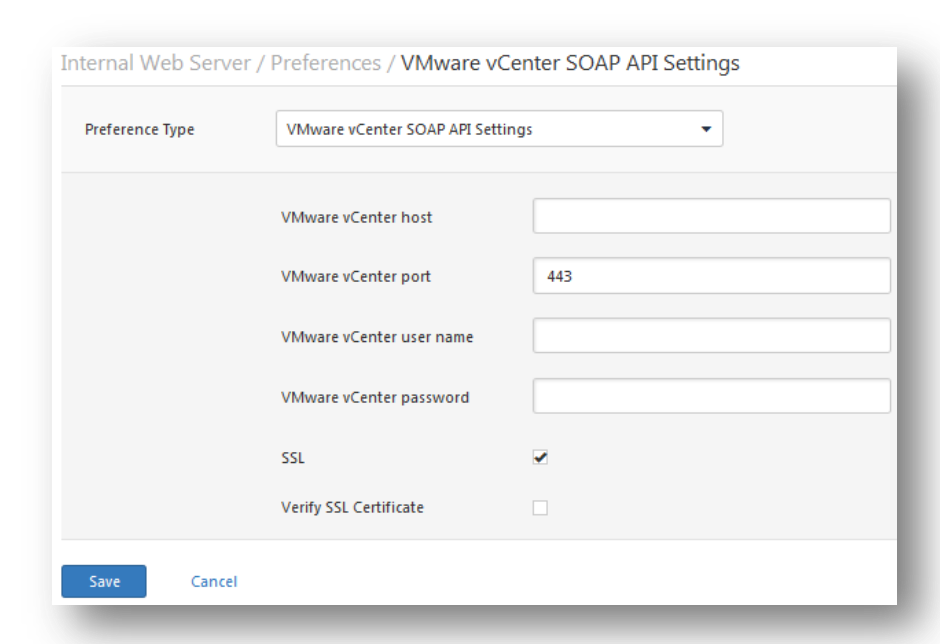
Das Menü „**VMware SOAP API Settings**" („Einstellungen für VMware SOAP-API") übergibt Nessus die Anmeldedaten, die erforderlich sind, um die Managementsysteme VMware ESX, ESXi und vSphere Hypervisor über die eigene SOAP-API zu authentifizieren (der SSH-Zugriff ist mittlerweile veraltet). Die API ist für Audits von vSphere 4.x-/5.x-, ESXi- und ESX-Hosts vorgesehen, jedoch **nicht** für auf den Hosts ausgeführte virtuelle Systeme. Mithilfe dieser Authentifizierungsmethode können authentifizierte Scans oder Compliance-Audits durchgeführt werden.



Option	Beschreibung
VMware user name (VMware-Benutzername)	Der für die Authentifizierung verwendete Benutzername. Bei integrierten Hosts oder lokalen Konten können die Anmeldedaten Active Directory-Konten sein, wobei sich das Konto in der lokalen Gruppe `root` befinden muss. Domänenanmeldedaten haben das Format „Benutzer@Domäne“, während bei lokalen Konten Benutzername und Kennwort angegeben werden müssen.
VMware password (unsafe!) (VMware-Kennwort – unsicher!)	Dieses Kennwort wird ungeschützt versendet und kann im Netzwerk von Dritten abgefangen werden.
Ignore SSL Certificate (SSL-Zertifikat ignorieren)	Wenn auf dem Server ein SSL-Zertifikat vorhanden ist, wird dieses ignoriert.

VMware vCenter SOAP API Settings

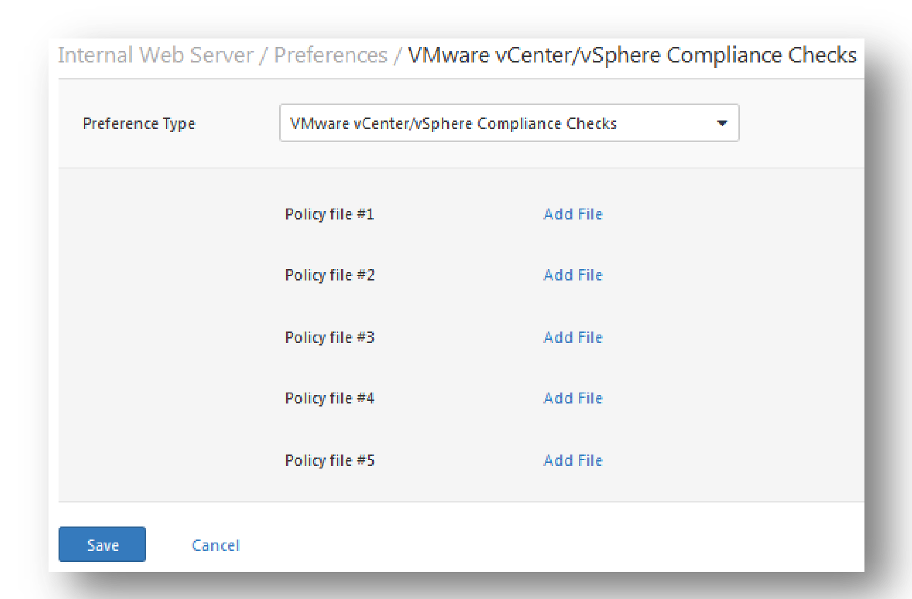
Das Menü „**VMware vCenter SOAP API Settings**“ („Einstellungen für VMware vCenter SOAP-API“) übergibt Nessus die Anmeldedaten, die erforderlich sind, um das VMware vCenter über die eigene SOAP-API zu authentifizieren (der SSH-Zugriff ist mittlerweile veraltet). Die API ist für Audits von vCenter vorgesehen, jedoch **nicht** für auf den Hosts ausgeführte virtuelle Systeme. Mithilfe dieser Authentifizierungsmethode können authentifizierte Scans oder Compliance-Audits durchgeführt werden.



Option	Beschreibung
VMware vCenter host (VMware vCenter-Host)	Hostname oder IP-Adresse der zu testenden vCenter-Installation.
VMware vCenter port (VMware vCenter-Port)	Port, auf dem vCenter antwortet (Standard: 443).
VMware user name (VMware-Benutzername)	Der für die Authentifizierung verwendete Benutzername. Bei integrierten Hosts oder lokalen Konten können die Anmeldedaten Active Directory-Konten sein, wobei sich das Konto in der lokalen Gruppe `root` befinden muss. Domänenanmeldedaten haben das Format „Benutzer@Domäne“, während bei lokalen Konten Benutzername und Kennwort angegeben werden müssen.
VMware vCenter password (VMware vCenter-Kennwort)	Dieses Kennwort wird ungeschützt versendet und kann, sofern SSL nicht angegeben wurde, im Netzwerk von Dritten abgefangen werden.
SSL	Verwenden Sie SSL für die Verbindung mit dem Host.
Verify SSL Certificate (SSL-Zertifikat bestätigen)	Wenn auf dem Server ein SSL-Zertifikat vorhanden ist, sollten Sie dessen Integrität prüfen.

VMware vCenter/vSphere Compliance Checks

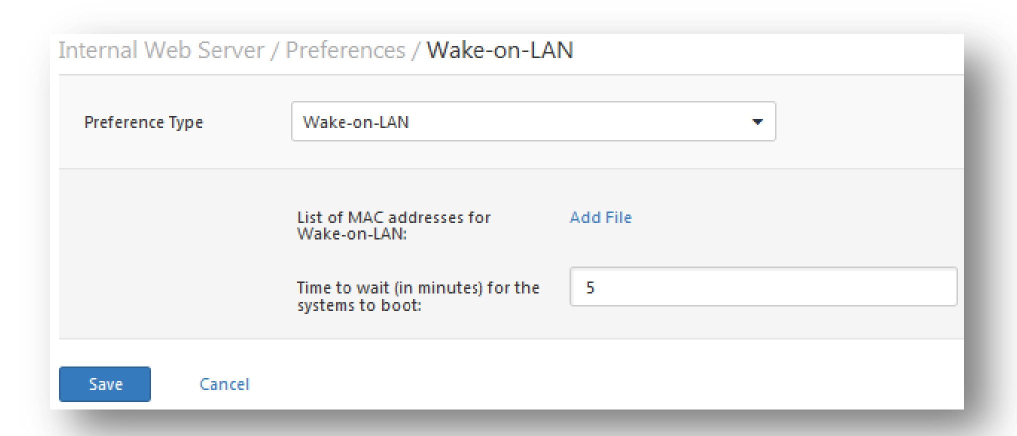
Das Menü „**VMware vCenter/vSphere Compliance Checks**“ („VMware vCenter/vSphere-Compliancetests“) ermöglicht es Benutzern der kostenpflichtigen Version, VMware vCenter- oder vSphere-Auditdateien hochzuladen, anhand derer ermittelt wird, ob ein getestetes System die angeforderten Compliancestandards erfüllt. Bis zu fünf Richtlinien können gleichzeitig ausgewählt werden.



Wake-on-LAN (WOL)

Im Menü „**Wake-on-LAN**“ wird festgelegt, an welche Hosts vor der Ausführung eines Scans WOL-Pakete übermittelt werden sollen und wie lange (in Minuten) auf den Start dieser Systeme gewartet werden soll. Die Liste der MAC-Adressen für die WOL-Funktion wird durch den Upload einer Textdatei festgelegt, in der jeweils eine MAC-Adresse pro Zeile aufgeführt ist. Beispiel:

```
00:11:22:33:44:55
aa:bb:cc:dd:ee:ff
[…]
```



Web Application Test Settings

Das Menü „**Web Application Tests Settings**“ („Einstellungen für Webanwendungstests“) testet die Argumente der Remote-CGIs (Common Gateway Interface), die beim Webspiegelungsprozess erkannt wurden. Hierzu wird versucht, verbreitete CGI-Programmierfehler wie Cross-Site Scripting, Remote File Inclusion, Befehlsausführung, Traversal-Angriffe oder SQL Injection zu übergeben. Sie aktivieren diese Option durch Markierung des Kontrollkästchens „Enable web applications tests“ („Webanwendungstests aktivieren“). Diese Tests erfordern die folgenden NASL-Plugins:

- 11139, 42424, 42479, 42426, 42427, 43160 – SQL Injection (CGI-Missbrauch)

- 39465, 44967 – Befehlsausführung (CGI-Missbrauch)
- 39466, 47831, 42425, 46193, 49067 – Cross-Site Scripting (CGI-Missbrauch: XSS)
- 39467, 46195, 46194 – Directory Traversal (CGI-Missbrauch)
- 39468 – HTTP Header Injection (CGI-Missbrauch: XSS)
- 39469, 42056, 42872 – File Inclusion (CGI-Missbrauch)
- 42055 – Formatstring (CGI-Missbrauch)
- 42423, 42054 – Server Side Includes (CGI-Missbrauch)
- 44136 - Cookiemanipulation (CGI-Missbrauch)
- 46196 – XML Injection (CGI-Missbrauch)
- 40406, 48926, 48927 – Fehlermeldungen
- 47830, 47832, 47834, 44134 – Weitere Angriffe (CGI-Missbrauch)

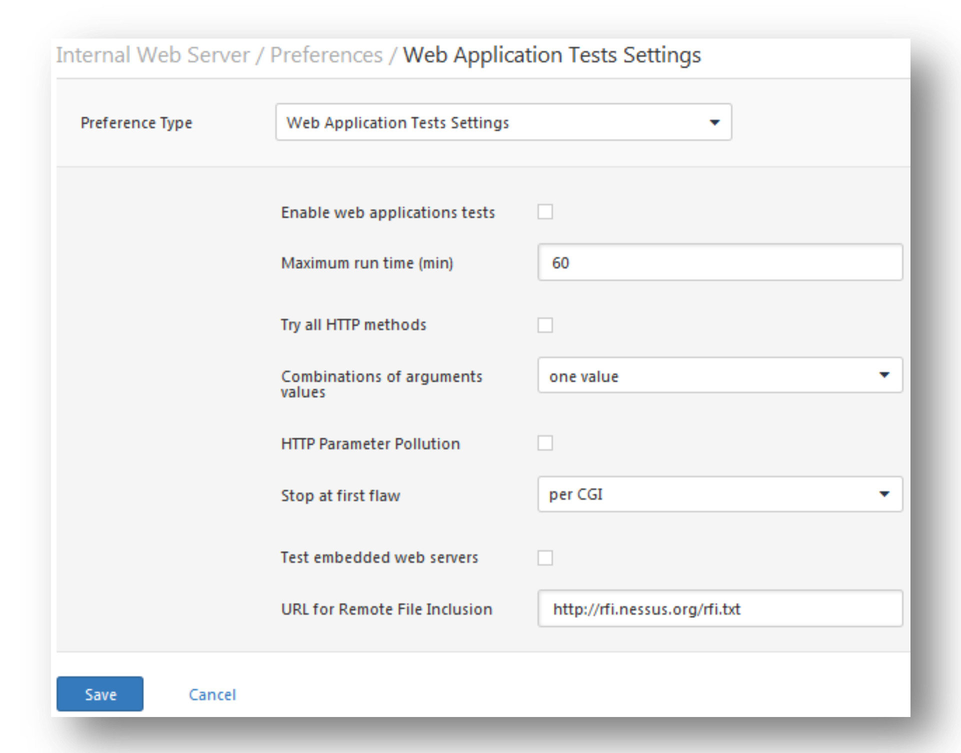


Hinweis: Diese Liste webanwendungsspezifischer Plugins wird regelmäßig aktualisiert. Sie kann unter Umständen unvollständig sein. Weitere Plugins können von den hier betroffenen Einstellungen abhängen.

Option	Beschreibung
Maximum run time (min) (Maximale Ausführungszeit in Min.)	Mithilfe dieser Option wird festgelegt, wie viel Zeit (in Minuten) für die Durchführung von Webanwendungstests aufgewendet werden darf. Die Vorgabe beträgt 60 Minuten und gilt für alle Ports und CGIs einer Website. Das Scannen des lokalen Netzwerks auf Websites mit kleineren Anwendungen wird in der Regel innerhalb einer Stunde abgeschlossen, doch kann für Websites mit umfangreichen Anwendungen ein höherer Wert erforderlich sein.
Try all HTTP methods (Alle HTTP-Methoden ausprobieren)	Standardmäßig testet Nessus nur unter Verwendung von GET-Anforderungen. Mithilfe dieser Option wird Nessus angewiesen, auch POST-Anforderungen zu verwenden, um die Überprüfung von Webformularen zu verbessern. Standardmäßig werden bei Webanwendungstests nur GET-Anforderungen verwendet, sofern diese Option nicht aktiviert ist. Im Allgemeinen verwenden komplexere Anwendungen die POST-Methode, wenn ein Benutzer Daten an die Anwendung übermittelt. Diese Einstellung ermöglicht umfassendere Tests, kann die erforderliche Zeit jedoch erheblich verlängern. Wird sie ausgewählt, dann testet Nessus jedes Skript und jede Variable sowohl mit GET- als auch mit POST-Anforderungen.
Combinations of arguments values (Kombinationen aus Argumentwerten)	Diese Option verwaltet die Kombination von Argumentwerten, die in HTTP-Anforderungen verwendet werden. Das Dropdownmenü enthält drei Optionen: „**One value**“ („Bestimmter Wert“): Hiermit wird immer nur ein Parameter gleichzeitig mit einem Angriffsstring getestet. „Angriffslose“ Varianten für weitere Parameter werden nicht ausprobiert. Beispielsweise würde Nessus „`/test.php?arg1=XSS&b=1&c=1`“ ausprobieren, wobei „b“ und „c“ andere Werte gestatten würden, ohne dass jede einzelne Kombination überprüft würde. Dies ist die schnellste Testmöglichkeit, bei der zudem die kleinste Ergebnismenge erzeugt wird. „**All pairs (slower but efficient)**“ („Alle Paare (langsamer, aber wirksamer)“): Dieser

	Testansatz ist etwas langsamer, aber wirksamer als der „One value"-Test. Beim Testen mehrerer Parameter werden ein Angriffsstring und Varianten für eine einzelne Variable getestet, und der erste Wert wird dann für alle anderen Variablen verwendet. Beispielsweise würde Nessus „`/test.php?a=XSS&b=1&c=1&d=1`" ausprobieren und die Variablen dann nacheinander so abarbeiten, dass einer Variable der Angriffsstring übergeben wird, einer weiteren zyklisch alle möglichen Werte übergeben werden (wie sie beim Spiegelungsprozess ermittelt wurden) und alle anderen Variablen den ersten Wert erhalten. In diesem Fall würde Nessus niemals auf „`/test.php?a=XSS&b=3&c=3&d=3`" prüfen, wenn der erste Wert jeder Variable „1" wäre. „**All combinations (extremely slow)**" („Alle Kombinationen (extrem langsam)"): Bei dieser Testmethode wird ein umfassender Test aller möglichen Kombinationen von Angriffsstrings mit gültigen Eingabewerten für die Variablen ausgeführt. Hierbei wird bei „All-pairs" („Alle Paare") zur Geschwindigkeitssteigerung versucht, eine kleinere Datenmenge zu erstellen, während bei „All combinations" („Alle Kombinationen") kein Kompromiss eingegangen wird – hier wird die gesamte Datenmenge für Tests verwendet. Beachten Sie, dass der Abschluss des Vorgangs bei dieser Testmethode **sehr lange** dauern kann.
HTTP Parameter Pollution	Beschreibt bei der Durchführung von Webanwendungstests den Versuch, vorhandene Filtermechanismen zu umgehen. Hierzu werden Inhalte in eine Variable injiziert, während gleichzeitig dieselbe Variable mit gültigem Inhalt übergeben wird. Ein normaler SQL-Injection-Test könnte etwa so aussehen: „`/target.cgi?a='&b=2`". Mit aktivierter HTTP Parameter Pollution (HPP) sähe die Anforderung dann eher so aus: „`/target.cgi?a='&a=1&b=2`".
Stop at first flaw (Bei erstem Schwachpunkt anhalten)	Mit dieser Option wird bestimmt, wann ein neuer Schwachpunkt als Ziel verwendet wird. Dies betrifft die Skriptebene: Die Erkennung eines XSS-Schwachpunkts führt nicht zu einer Deaktivierung der Suche nach SQL-Injection- oder Header-Injection-Schwachpunkten; allerdings erhalten Sie maximal einen Bericht zu jedem Typ auf dem jeweiligen Port, sofern „Thorough tests" („Umfassende Tests") nicht festgelegt ist. Beachten Sie, dass mehrere Schwachpunkte desselben Typs (z. B. XSS, SQLi usw.) gemeldet werden können, sofern sie vom selben Angriff erfasst wurden. Das Dropdownmenü enthält vier Optionen: „**Per CGI**" („Je CGI"): Sobald ein Schwachpunkt von einem Skript in einem CGI gefunden wurde, wechselt Nessus zum nächsten bekannten CGI auf demselben Server bzw. – wenn kein CGI mehr vorhanden ist – zum nächsten Port oder Server. Dies ist die Grundeinstellung. „**Per port (quicker)**" („Je Port (schneller)"): Sobald ein Schwachpunkt von einem Skript auf einem Webserver gefunden wurde, stoppt Nessus und wechselt zu einem anderen Webserver auf einem anderen Port. „**Per parameter (slow)**" („Je Parameter (langsam)"): Sobald ein Schwachpunkttyp (z. B. XSS) in einem CGI gefunden wurde, wechselt Nessus zum nächsten Parameter desselben CGI, zum nächsten CGI oder zum nächsten Port oder Server. „**Look for all flaws (slower)**" („Nach allen Schwachpunkten suchen (langsamer)"): Führt umfassende Tests unabhängig von den gefundenen Schwachpunkten durch. Diese Option kann einen sehr ausführlichen Bericht generieren. In den meisten Fällen ist von ihrer Verwendung abzuraten.
Test Embedded web servers (Eingebettete	Eingebettete Webserver sind häufig statisch und enthalten keine anpassbaren CGI-Skripts. Zudem sind eingebettete Webserver möglicherweise absturzanfällig oder

Webserver testen)	reagieren beim Scannen nicht mehr. Tenable empfiehlt das Scannen eingebetteter Webserver separat von anderen Webservern mithilfe dieser Option.
URL for Remote File Inclusion (URL für Remote File Inclusion)	Beim RFI-Test (Remote File Inclusion) gibt diese Option eine Datei auf einem Remotehost an, die für die Tests verwendet wird. Standardmäßig benutzt Nessus eine sichere Datei, die auf dem Webserver von Tenable gehostet und speziell für RFI-Tests vorgesehen ist. Kann der Scanner nicht auf das Internet zugreifen, dann wird die Verwendung einer intern gehosteten Datei für genauere RFI-Tests empfohlen.



Web mirroring

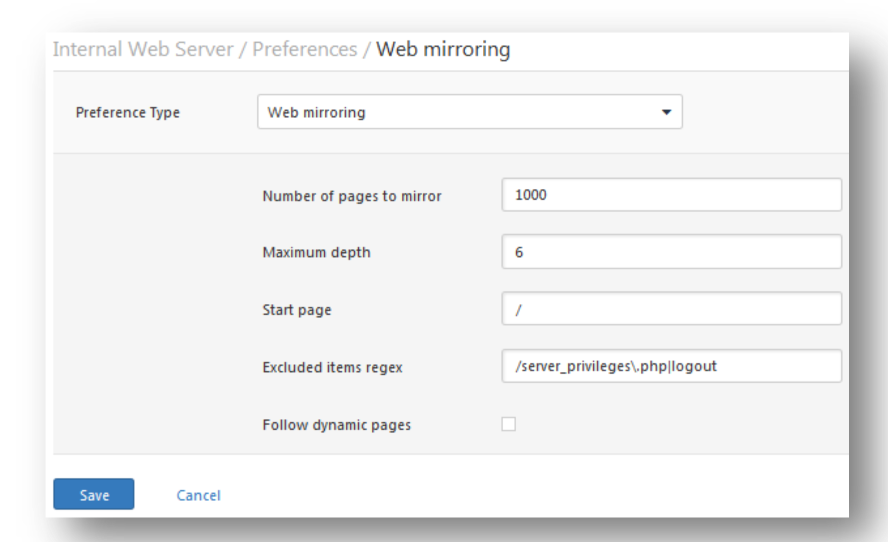
Mit dem Menü „**Web Mirroring**“ („Webspiegelung“) werden Konfigurationsparameter für das native Nessus-Utility zur Spiegelung von Webserverinhalten festgelegt. Nessus spiegelt Webinhalte, um sie besser auf Sicherheitslücken prüfen zu können und die Auswirkungen auf den Server zu minimieren.



Wenn die Webspiegelungsparameter so festgelegt sind, dass eine vollständige Website gespiegelt wird, kann dies zu erheblichem Datenaufkommen während des Scans führen. Ist beispielsweise 1 GB Daten auf einem Webserver vorhanden und wurde Nessus so konfiguriert, dass alles gespiegelt wird, so wird beim Scan auch mindestens 1 GB Datenverkehr vom Server zum Nessus-Scanner generiert.

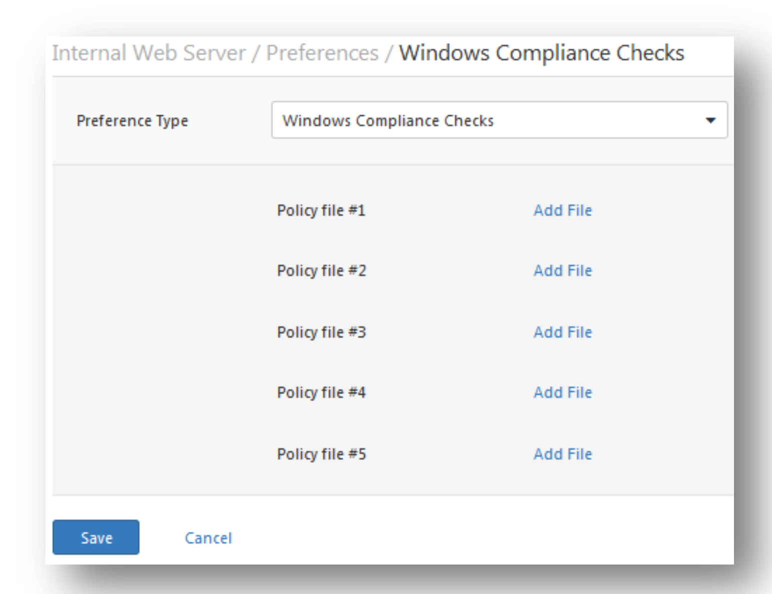
Option	Beschreibung
Number of pages to mirror (Anzahl zu spiegelnder Seiten)	Maximale Anzahl zu spiegelnder Seiten.
Maximum depth (Maximale Spiegelungstiefe)	Hiermit wird angegeben, wie vielen Links Nessus je Startseite folgt.

Start page (Startseite)	URL der ersten zu testenden Seite. Sind mehrere Seiten erforderlich, dann können diese durch einen Doppelpunkt getrennt angegeben werden (z. B. „/:/php4:/base“).
Excluded items regex (Regulärer Ausdruck für ausgeschlossene Elemente)	Hiermit wird der Ausschluss von Teilen der erfassten Website aktiviert. Um beispielsweise das Verzeichnis „/manual“ und alle Perl-CGIs auszuschließen, geben Sie folgenden Wert für dieses Feld an: `(^/manual)|(\.pl(\?.*)?$)`.
Follow dynamic pages (Dynamischen Seiten folgen)	Wenn diese Option aktiviert ist, folgt Nessus dynamischen Links, wodurch die oben festgelegten Grenzwerte überschritten werden können.



Windows Compliance Checks

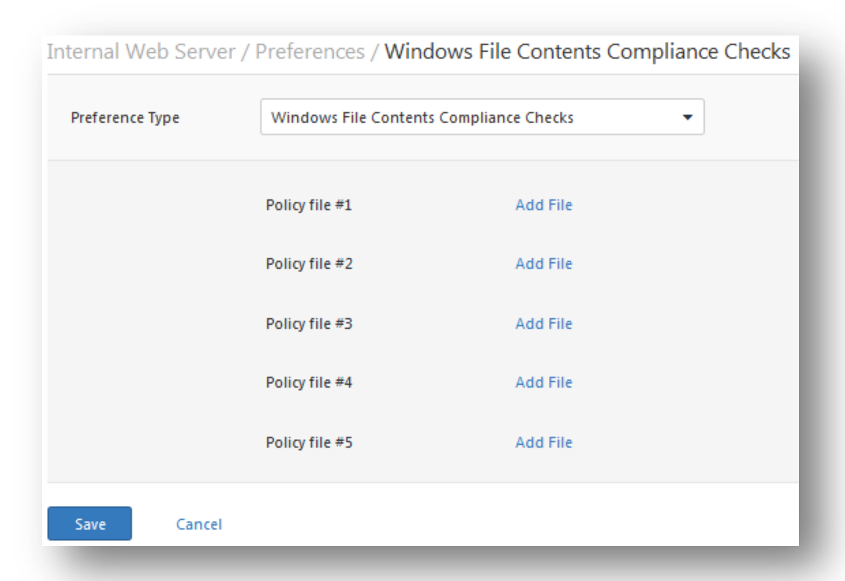
Mit dem Menü „**Windows Compliance Checks**“ („Windows-Compliancetests“) können Benutzer der kostenpflichtigen Version Microsoft Windows-Konfigurationsauditdateien hochladen, anhand derer ermittelt wird, ob ein getestetes System die angeforderten Compliancestandards erfüllt. Bis zu fünf Richtlinien können gleichzeitig ausgewählt werden.



Windows File Contents Compliance Checks

Mit dem Menü „**Windows File Contents Compliance Checks**" („Windows-Compliancetests für Dateiinhalte") können Benutzer der kostenpflichtigen Version Windows-basierte Auditdateien hochladen, die nach bestimmten Inhaltstypen suchen (z. B. Kreditkartennummern, Social Security-Nummern usw.), und so die Compliance in Bezug auf Unternehmensrichtlinien oder Drittvorgaben bestimmen.

Wenn alle Optionen wie gewünscht konfiguriert wurden, klicken Sie auf „**Submit**" („Senden"), um die Richtlinie zu speichern und zur Registerkarte „Policies" („Richtlinien") zurückzukehren. Sie können jederzeit auf „**Edit**" („Bearbeiten") klicken, um Änderungen an einer Richtlinie vorzunehmen, die Sie bereits erstellt haben. Durch Anklicken von „**Delete**" („Löschen") löschen Sie eine Richtlinie vollständig.



Weitere Informationen

Tenable hat eine Reihe von Dokumenten erstellt, in denen die Bereitstellung, die Installation, die Konfiguration, der Betrieb und die Testmethoden von Nessus ausführlich beschrieben werden. Es sind diese:

- **Nessus 5.2 Installation and Configuration Guide** („Nessus 5.2-Installations- und Konfigurationshandbuch“; Schrittanleitung zur Nessus-Installation und -Konfiguration)
- **Nessus Credential Checks for Unix and Windows** („Authentifizierte Nessus-Tests für UNIX und Windows“; enthält Informationen zur Durchführung authentifizierter Netzwerkscans mit dem Nessus-Sicherheitslückenscanner)
- **Nessus Compliance Checks** („Nessus-Compliancetests“; allgemeiner Leitfaden zum Verständnis und zur Durchführung von Compliancetests mithilfe von Nessus und SecurityCenter)
- **Nessus Compliance Checks Reference** („Nessus-Referenzhandbuch für Compliancetests“; umfassender Leitfaden zur Syntax von Nessus-Compliancetests)
- **Nessus v2 File Format** („Nessus V2-Dateiformat“; beschreibt die Struktur des **`.nessus`**-Dateiformats, das mit Nessus 3.2 und NessusClient 3.2 eingeführt wurde)
- **Nessus 5.0 REST Protocol Specification** („Nessus 5.0 REST-Protokollspezifikation“; beschreibt das REST-Protokoll und die Schnittstelle in Nessus)
- **Nessus 5 and Antivirus** („Nessus 5 und Virenschutz“; beschreibt die Funktion verschiedener gängiger Sicherheitssoftwarepakete in Nessus und enthält Tipps und Lösungsvorschläge für eine verbesserte Funktionsweise der Software ohne Einschränkung der Sicherheit oder Verhinderung Ihrer Sicherheitslückenscans)
- **Nessus 5 and Mobile Device Scanning** („Nessus 5 und Scans von Mobilgeräten“; beschreibt die Integration von Nessus in Microsoft Active Directory und Verwaltungsserver für Mobilgeräte zur Bestimmung von im Netzwerk eingesetzten Mobilgeräten)
- **Nessus 5.0 and Scanning Virtual Machines** („Nessus 5.0 und Scans virtueller Maschinen“; beschreibt den Einsatz des Sicherheitslückenscanners von Tenable Network Security Nessus für Audits der Konfiguration virtueller Plattformen sowie der darauf ausgeführten Software)
- **Strategic Anti-malware Monitoring with Nessus, PVS, and LCE** („Strategische Malwareüberwachung mit Nessus, PVS und LCE“; beschreibt, wie mithilfe der Tenable USM-Plattform zahlreiche bösartige Softwareprogramme erkannt werden können und das Ausmaß der Malware-Infizierung bestimmt werden kann)
- **Patch Management Integration** („Integration des Patchmanagements“; beschreibt, wie Nessus und SecurityCenter mithilfe von Berechtigungen auf die IBM TEM-, Microsoft WSUS- und SCCM-, VMware Go- und Red Hat Network Satellite-Patchmanagementsysteme Patch-Audits auf Systemen ausführen, für die dem Nessus-Scanner möglicherweise keine Berechtigungen zur Verfügung stehen)
- **Real-Time Compliance Monitoring** („Compliance-Überwachung in Echtzeit“; erläutert, wie die Lösungen von Tenable Sie bei der Erfüllung zahlreicher gesetzlicher Vorschriften und Finanzstandards unterstützen)
- **Tenable Products Plugin Families** („Tenable Produkt-Plugin-Familien“; stellt eine Beschreibung und Zusammenfassung der Plugin-Serien für Nessus, Log Correlation Engine und den Passive Vulnerability Scanner bereit)

- **SecurityCenter Administration Guide** („SecurityCenter-Administratorhandbuch“)

Weitere Onlineressourcen sind nachfolgend aufgeführt:

- Nessus-Diskussionsforum: https://discussions.nessus.org/
- Tenable-Blog: http://www.tenable.com/blog
- Tenable-Podcast: http://www.tenable.com/podcast
- Beispielvideos zum Gebrauch: http://www.youtube.com/user/tenablesecurity
- Tenable-Twitterfeed: http://twitter.com/tenablesecurity

Setzen Sie sich mit uns in Verbindung – via E-Mail (support@tenable.com, sales@tenable.com) oder über unsere Website unter http://www.tenable.com/.

Wissenswertes zu Tenable Network Security

Wenn es um die frühzeitige Erkennung neu entwickelter Sicherheitslücken, Bedrohungen und Compliance-relevanter Risiken geht, verlassen sich mehr als 20.000 Organisationen auf Tenable Network Security. Hierzu gehören neben dem gesamten US-Verteidigungsministerium eine Reihe von Großunternehmen und Regierungsbehörden weltweit. Die Nessus- und SecurityCenter-Lösungen sind nach wie vor branchenführend beim Ermitteln von Sicherheitslücken, beim Verhindern von Angriffen und bei der Erfüllung einer Vielzahl gesetzlicher Vorschriften. Weitere Informationen finden Sie unter www.tenable.com.

GLOBALE UNTERNEHMENSZENTRALE

Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046, USA
+1.410.872.0555
www.tenable.com

